Letters, Power Lines, and Other Dangerous Things

The Politics of Infrastructure Security

The title-level DOI for this work is:

doi:10.7551/mitpress/10541.001.0001

3

Imagination Unbound: Risk, Politics, and Post-9/11 Anxiety

Life is good in America because things work.
—President's Commission on Critical Infrastructure Protection, 1997[1]

Infrastructures have *always* been dangerous. In the late 1870s, the Post Office Department's annual reports included a grim annex—a listing of casualties. Across several pages of small type, the Post Office Department's superintendent for Railway Mail Service provided accounts of the postal workers killed or maimed while transporting the mail by railroad. In 1878, General Superintendent of the Railway Mail Service (and future president of American Telephone & Telegraph [AT&T]) Theodore Vail offered a bleak introduction to the table of casualties:

> The following list of casualties will give some approximate idea of the continual risk to which the employés of this service were exposed; hardly a week passes but some employé is killed, oftentimes in the most horrible manner—maimed for life, which is worse—or so injured that for weeks and months he can perform no service.[2]

Vail recorded various train derailments, crashes, fires, and other accidents that affected both postal workers and the mail. He mixed accounts of bodily harm with descriptions of the impact of the accidents on the mail. The entry for September 21, 1878, is instructive:

> *September* 21.—New York, Central and Hudson River Railroad, Chicago express, collided with freight-train near Rome, N.Y. Both engines, mail, and baggage-cars completely wrecked. Head Clerk John S. Tunnard, and a fireman and brakeman killed, and Postal Clerks Frank O. Roberts, George W. Fitch, William E. Earle, and William H.S. Sweet Seriously injured as were many railroad employés and passengers.
>
> Some of the registered matter was badly mutilated, but no mail known to be lost.[3]

The postal system—and the rail system—of the late 19th century was dangerous. It was hazardous to both the workers who helped move the

mail and the messages—letters and other postal ephemera—that flowed through the sinews of the system. Postal clerks often died, lost limbs, and faced other serious ailments in the course of their jobs. To them, the postal system was certainly a dangerous place. And, as Vail's account makes plain, postal managers were acutely aware of these risks. Vail was writing in part to advocate for pensions and other benefits for injured workers.[4]

The postal system, freight rail network, and electric power grid have—to some—always been dangerous. For centuries, local communities feared that mail could spread disease. At different points in time, letters were taken to be carriers of plague, cholera, yellow fever, and a host of other maladies.[5] These fears led to baroque practices of postal disinfection, including specialized fumigation devices, a complex array of markings certifying the "health" of the mail, envelopes specifically designed to allow for cleaning, and disinfection stations.[6] More blunt techniques were also used. During epidemics of yellow fever, shotgun-wielding bands of worried locals would refuse to allow railcars carrying mail that arrived from areas where the disease was present to stop and unload.[7] Railroads were also feared: rail accidents were spectacular and frequent occurrences for much of the first century of railroading.[8] These accidents were staples of mid- and late-19th century newspapers and subjects of popular concern.[9] Charles Dickens remarked on the horrors of American rail travel during his visit to the U.S.[10] For many, electricity remains worrisome: to a home filled with young children, electrical outlets remain an acute source of danger. A curious finger can result in an unwanted lesson in electrocution. "Toddler-proofing," the ritual transformation of an area into a place more suitable for kids, often includes placing cheap plastic covers over each outlet in order to lessen this risk.

In a sense, infrastructures *have always been dangerous*. Different publics relate to infrastructures in different ways. To some, these sociotechnical systems have always been imbued with hazard; to others, these systems are benign. Sometimes arguments about infrastructural risk are marginal—a minority opinion that is ignored. Other times, these ideas become powerful. They are adopted and translated into new policies, laws, technologies, and practices. They, in short, lead to infrastructural transformation.

* * * *

Part I of this book detailed how deregulation pushed infrastructures into newly vulnerable configurations. These material changes made new types of large-scale failure possible. But the identification and prioritization of

these systems as public problems required a larger cultural context that would make claims about infrastructure insecurity legible; it required institutions that would legitimize, accept, and act on these claims; and it required a set of organizations that would argue and push for new forms of infrastructure protection and security as a goal. Material changes on their own are worth little. Many things are potentially dangerous—risk resides nearly everywhere you look. Making a particular source of risk salient, elevating *this particular problem* into something that captures the public imagination, and placing this risk over all of the others that compete for attention and attending is not automatic. It is a social process that is inseparably bound with the material world.

In this respect, post-9/11 changes were crucial. The terrorist attacks of 9/11 were a profound tragedy. Terrorism quickly moved to the center of both foreign and domestic affairs in the U.S. It became—and nearly two decades later largely remains—a dominate prism through which to view and evaluate domestic security and international law and policy.[11] In remarks on September 11, 2001, President George W. Bush declared that America and its allies would be united in a "war against terrorism."[12] This war—fought not against a single enemy or nation but a more sweeping and expansive confrontation with a form of political violence—would justify myriad legal and policy transformations in the coming years.

President Bush quickly prioritized infrastructure security and protection as key elements of a newly launched homeland security strategy after 9/11. The global war on terror became a powerful lens through which to interpret all manner of topics, including infrastructure. The government suddenly embraced and elevated ideas about infrastructure vulnerability that had circulated with little currency in the prior five decades. This prioritization of infrastructure security by the Bush administration legitimized the cultural framing of infrastructures as dangerous objects in need of taming. Now, arguments that took as their starting point the vulnerability of infrastructure and the possibility of terrorist attack made sense—they were culturally intelligible and seen as legitimate. This cultural shift was backed by a set of supporting institutional changes: billions of dollars would soon become available for infrastructure security at the federal and state level; a new department—the Department of Homeland Security—would have infrastructure protection and security as one of its key charges; at every level of government, "security" would soon become a familiar and accepted way of directing the thinking about infrastructure. Organized interest groups and newly formed political coalitions would adopt the language of security and the war on terror to argue

for infrastructure reforms. Now, a host of organizations could put forward claims about infrastructure security and find audiences and venues that accepted these arguments and, importantly, resources to address these concerns. The material changes that deregulation ushered in mattered: they created new possibilities of failure. But it was only thanks to the overlapping cultural, institutional, and organizational shifts and reorientations that occurred after 9/11, that these changes were transformed into public problems.

This book now turns to map how the postal system, freight rail network, electric power grid, and other infrastructures were reframed as "dangerous things" in the wake of 9/11 and considers how in the years that followed new security interventions remade the material and organizational foundations of these infrastructures. The previous chapters examined the upheavals and transformations of deregulation. Viewed through the lens of the unfolding war on terrorism, these changes are now reframed and reinterpreted as public problems. The long-presumed virtues of deregulation—lean and efficient networks unencumbered by "meddlesome" regulation—appear in this new light to be vices. In the long post-9/11 moment, the celebrated successes of decades of deregulation are thrown into serious question. Contemporary infrastructure security debates wrestle with an uncomfortable reality: deregulation created networks prone to large-scale failure and, at the same time, it largely delegitimized public accountability and stewardship over infrastructure in favor of the free hand of the market. As policymakers and a cross-section of civil society groups began to consider how to make infrastructures secure in the days and years after 9/11, deregulation implicitly and explicitly went on trial.

This chapter charts how *critical infrastructure protection* emerged as a key governmental concern in the months and years after 9/11. This shift—rooting infrastructure within the larger realm of geostrategic conflicts and discussions of national or homeland security—was not a given. Rather, it resulted from deliberate policy decisions made at the highest levels of government. This chapter provides a window into how critical infrastructure protection moved from being a little-discussed topic of concern, hidden safely in obscure government reports and the little-read musings of DC think tanks into a taken-for-granted way of thinking about infrastructure. This shift set the stage for the conflicts over infrastructure governance that were to come.

In order to sort through this reframing, the second half of the chapter dives into a theoretical discussion about the political possibilities—and limitations—of risk. The work of Ulrich Beck and others set up an

interesting debate: Can risks spark democratic engagement? Can they serve as the foundation for new forms of collective action that challenge the sunk politics buried within the organization of infrastructure? Or are risks, inevitably, an ally of the powerful—a cudgel used to blunt attempts to democratize infrastructure? The subsequent chapters of the book flesh out this theoretical discussion by examining how organized interests took advantage of the threat of terrorism to remake and refashion the postal system, freight rail network, and electric power system.

Ubiquitous Targets: Rethinking and Reframing Infrastructure

In the days that followed the terrorist attacks of September 11, infrastructure security became a key national priority. Infrastructures often hide in plain sight—when they work, most people almost never think about them. As long as the lights stay on, water flows from the tap, and our shipments from Amazon arrive (nearly) on time, most of us waste little thought on the complex web of systems that make the conveniences of day-to-day life possible. After 9/11, however, infrastructures became newly visible. Policy-makers were chastised for failing to prevent the atrocities of 9/11. The National Commission on Terrorist Attacks upon the United States ("the 9/11 Commission") memorably described the systematic failure of the U.S. government to prevent the attacks as "a failure of imagination."[13] In post-9/11 America, imagination was unbound. Policy-makers, operators, and the public began to see terror lurking *everywhere*: wastewater systems, bridges, shipments of hazardous materials, the electric power grid, and even the postal system appeared to be possible targets. Terrorism made the familiar appear sinister. Infrastructures—the dull and boring systems that comprise the background wiring of modern life—were quickly and anxiously foregrounded as sites of vulnerability and fear. They were transformed in the public imagination into "dangerous things" and pulled firmly into the ambit of national security.

The recasting of infrastructures was driven by the highest reaches of the federal government. President Bush quickly placed infrastructure protection at the center of his domestic security agenda. On October 8, Bush signed an executive order creating the Office of Homeland Security within the White House and establishing a new interagency Homeland Security Council.[14] On the same day, the president named former Pennsylvania governor Tom Ridge as the first director of the office.[15] In remarks made during Ridge's swearing in ceremony, Bush noted that infrastructure protection would be one of the core missions of the new office and that the

office would seek to "strengthen and help protect our transportation systems, our food and water systems, and our *critical infrastructure* by making them less vulnerable to attack."[16] Pointedly, Bush framed infrastructure protection in expansive terms—arguing that the challenge of homeland security called for the protection of a range of disparate networks and systems that could be yoked together under the fuzzy rubric of *critical infrastructure*.[17] Rather than interpreting the terrorist attacks narrowly—focusing only on airline security, the infrastructure most directly relevant to the attack—the threat, in Bush's view, called for a larger rethinking of infrastructure. The executive order put the Office of Homeland Security in charge of coordinating efforts to protect infrastructure from the consequences of a terrorist attack.[18] It identified particular infrastructures for attention, highlighting transportation, energy, and telecommunications systems while also broadening the scope of what infrastructures would be included by adding the undefined term *critical infrastructure*.[19]

In late October, President Bush signed the USA PATRIOT Act of 2001 into law.[20] The law was sweeping, touching on surveillance reform, compensation for victims of terrorist attacks, and other areas or counterterrorism law.[21] It also defined critical infrastructure. Section 1016 of the act, known as the Critical Infrastructure Protection Act of 2001, defined critical infrastructure 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, national public health or safety, or any combination of those matters."[22] The law, however, provided little in the way of new authorities or funding for infrastructure protection: just a modest $20 million for the creation of a new infrastructure analysis center within the Defense Threat Reduction Agency.[23] The new law affirmed that the policy of the U.S. was to ensure that any and all disruptions to infrastructure be "brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States."[24] This language was important. It made it clear that infrastructures were now being viewed through the lens of security concerns (as a core part of an emerging definition of *homeland security*). Yet the Patriot Act and the executive order establishing the Office of Homeland Security said little about what, exactly, was to be done. How the U.S. would precisely go about securing the various transportation, power, telecommunication, and other networks that might be included in the category of critical infrastructure was very much an open question. What form these new security interventions would eventually take, their impact, and their

significance would be decided in the years to come through contentious and bitter negotiation and maneuvering. Infrastructure security was now, at least symbolically, a key front in the war on terror. The implications of this recasting, however, were still unknown.

The Cultural Construction of Infrastructure Vulnerability: A Partial History

The reframing of infrastructures as dangerous objects began immediately after the attacks of 9/11. But, this recasting rested on a deep foundation. Part I of the book charted the material and historical foundations of infrastructure vulnerability. Political and economic changes in how infrastructures are governed introduced new forms of vulnerabilities and new possibilities for failure. Yet this is only part of the story. These vulnerabilities and risks were not necessarily obvious. Risks never speak for themselves. That these risks, these vulnerabilities, and these systems—as opposed to others—would in time be identified and fashioned into public problems was not inevitable. On the contrary, it required a particular type of vision, a particular way of understanding and making sense of infrastructures, to transform these networks into topics of public concern. In this fashion, infrastructure risk was *coproduced*—it sat at the intersection of material and cultural change.[25] The cultural redefinition of infrastructures as dangerous objects did not appear out of thin air. In those early days after 9/11, Bush and the administration drew from and built on ideas and cultural constructions that had been gestating at the margins with little attention and little currency for decades. As Andrew Lakoff, Stephen Collier, and Eric Klinenberg have expertly mined, there is a rich genealogy beneath the contemporary rush to consider infrastructure as a national security problem.[26] Working during the Cold War and immediate post–Cold War period, policy-makers and defense thinkers began to articulate a set of concerns and a way of thinking about infrastructure that would come to dominate post-9/11 politics. In a series of little-read research reports and policy documents, these groups sketched out concerns over the increasing brittleness of civilian infrastructure, the impact that computerization might have on infrastructure vulnerability, and, most significantly, the ways in which terrorists might exploit infrastructures to cause significant economic disruption and, possibly, loss of life. Before 9/11 these ideas were marginal and received little traction (either inside the government or outside). After 9/11, they became ascendant. They offered a vocabulary for thinking about infrastructure that would

become commonplace. Although the various policy wonks, researchers, and government officials that fashioned these concepts in relative obscurity during the second half of the 20th century could not have realized it at the time, these ideas would provide the conceptual foundations for the most significant restructuring of the federal government since 1947.[27]

Infrastructure protection was a recurring, though decidedly minor, theme during the Cold War and immediate post–Cold War period.[28] Cold War civil defense efforts focused in part on strategies to protect infrastructure from military strike. In the 1950s and 1960s, a rotating cast of governmental bodies tackled the issue of infrastructure security. The National Security Resource Board (NSRB), the Federal Civil Defense Administration, the Business and Defense Services Administration, the Office of Defense Mobilization, and a host of other long-forgotten organizations sounded the alarm for infrastructure security.[29] As schoolchildren practiced duck-and-cover drills, these bodies focused on the brittleness of the U.S. energy, communication, manufacturing, and transportation systems in response to a military strike. U.S. Cold War strategy rested on three pillars: containment, deterrence, and preparedness.[30] Preparedness had its own grim logic: It suggested that a Soviet attack was all but inevitable. Therefore, key infrastructure systems should be made sustainable in order to survive a military attack.[31] A steady stream of governmental reports pointed out the challenges of infrastructure vulnerability—often with little noticeable impact. In the early 1960s, the Defense Electric Power Administration released a report on the vulnerability of the electric power system.[32] Reports by the Government Accounting Office (GAO) and the Congressional Research Service (CRS) during the late 1970s and early 1980s warned that the U.S. pipeline system and electric power system were both susceptible to attack.[33] The ambition of these efforts exceeded their grasp. For example, the National Security Resource Board led an effort of *industrial dispersal*—a plan to limit the concentration of industrial facilities in particular geographic regions.[34] Spreading out key industrial facilities, the thinking went, would make military strikes against the U.S. less devastating. But moving industrial facilities away from population centers or important resources proved nearly impossible. As the NSRB's own chairman, Arthur Hill, noted, it was entirely impractical to attempt to break up or relocate the production of steel outside of Pittsburgh.[35]

In the 1970s an important pivot occurred. Planners started to move beyond an exclusive Soviet focus and consider a range of possible threats targeting infrastructure. The terrorist attacks during the Munich Olympics led the Nixon administration to create the Cabinet Committee to Combat

Terrorism and, subsequently, the Interagency Study Group to consider how to prevent and respond to international and domestic terrorism.[36] In the following years, the work of the study group looked beyond the boundaries of a Cold War confrontation and started to take seriously the possibility of a terrorist attack targeting transportation infrastructure, the electric power grid, or nuclear facilities.[37] It concluded that the risk of what it termed *intermediate terrorism*, attacks that did not rise to the level of mass destruction but were more consequential than a single abduction or assassination, deserved serious attention. A high-profile study conducted by the Center for Strategic and International Studies (CSIS) and cochaired by Robert H. Kupperman (the former head of the Interagency Study Group) and future CIA director R. James Woolsey attempted to push the topic of infrastructure security into the forefront of political conversation.[38] The report, *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks*, was blunt and explicit.[39] America's networks were targets in waiting. CSIS stated that infrastructures represent the "fragile fabric of our nation" and wrote:[40]

> U.S. national security vulnerabilities do not lie solely in the Middle East, or Western Europe, or Central America, or the Western Pacific. Inside the United States itself, we have grown dependent economically, technologically, and psychologically upon highly complex service networks for our well-being. The telephone, electric power system, oil and gas pipelines, railroads, ocean and river shipping, and highways have become integral parts of our lives. We have come to take these networks for granted … yet, these domestic networks … suffer from procedural and technical vulnerabilities to serious accidental or deliberate disruption. … We cannot withdraw even in theory from the U.S. electric power grid, the computer and telecommunications systems, or our internal transportation networks.[41]

The CSIS group was direct: infrastructure vulnerability was a key national security challenge; the networks that the nation relied on were vital and brittle. The report, much like those that had preceded it, made little impact.

The most significant foundation for the post-9/11 rise of infrastructure security was the work completed by the President's Commission on Critical Infrastructure Protection (PCCIP) in the mid-1990s. The PCCIP could not have predicted that its work would have a fate in any way different from the various reports and warnings that had been produced, to little effect, in the previous decades. Timing, however, was everything.

In the wake of the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, President Clinton signed Presidential Decision Directive 39 (PDD 39), "U.S. Policy on Counterterrorism."[42] The directive outlined U.S. counterterrorism policy and set the stage, indirectly, for the

creation of the PCCIP. The first section of PDD 39 was titled "Reducing Our Vulnerabilities."[43] The directive instructed the Department of Justice (DOJ) to convene a cabinet-level interagency group "to review the vulnerability to terrorism of government facilities in the United States and critical national infrastructure and make recommendations."[44] The day-to-day work was led by Deputy Attorney General Jamie Gorelick.[45] The working group—dubbed the Critical Infrastructure Working Group—considered both terrorism and natural disasters.[46] The phrase *critical infrastructure* stuck. It would become a catchall term for conversations about national security or homeland security challenges relating to infrastructure vulnerability moving forward. In its final report, the working group identified eight critical infrastructure sectors—telecommunications, electrical power, gas and oil, banking and finance, transportation, water supply, emergency services, and continuation of government—and recommended that President Clinton establish a commission to comprehensively review infrastructure security and identify legal and policy options to mitigate these challenges.[47] It was an evergreen and classic inside-the-Beltway recommendation: when faced with a sprawling problem with no clear, easy answer, recommend a commission to study the problem further. Who could possibly object to more study?

President Clinton signed Executive Order No. 13010, "Critical Infrastructure Protection," in July 1996.[48] The order created the PCCIP and defined *critical infrastructure* as those national infrastructures that "are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[49] The language would be picked up in subsequent reports and eventually added with some alteration to the Patriot Act. The order adopted the eight sectors that the Critical Infrastructure Working Group had defined and tasked the PCCIP with consulting with key public and private sector stakeholders; assessing the scope of threats and vulnerabilities that confront critical infrastructure; identifying key legal and policy issues raised by the challenges of infrastructure security; and recommending a comprehensive national strategy to secure critical infrastructure. The PCCIP was chaired by Robert Marsh, a retired U.S. Air Force general, and featured commissioners from both the private sector (AT&T, Pacific Gas and Electric, IBM, Association of American Railroads) and government (Federal Emergency Management Agency, Department of the Treasury, Department of Defense, Department of Energy, DOJ, Department of Commerce, National Association of Regulatory Commissioners, Federal Reserve Board, National Security Agency, CIA, and FBI).[50]

The PCCIP worked for a little over a year and released its final report, *Critical Foundations: Protecting America's Infrastructures*, in the fall of 1997. At first glance the report echoes the conversations that had percolated within various corners of the government for decades: America's infrastructures are both vital to modern society and vulnerable to attack. More interestingly, the report roots its concern over infrastructure vulnerability in the context of a shifting, technological, political, and even economic landscape—what it calls "the new geography."[51] The prevailing tenor of the report is *anxiety*—over new technology, over the loss of the predictable (if terrifying) logic and stability of the Cold War, and over the perils of open markets. In this respect the report very much reads like the mid-1990s document it is. It spends a substantial amount of time describing the novel challenge of what it refers to as "cyber-threats." The commission argues that the diffusion of information and communications technologies creates new complexity within and across infrastructures and new forms of interdependency that could be exploited.[52] The commission is blunt: "We … face the possibility that someone will be able to actually mount an attack against other infrastructures by exploiting their dependence on computers and telecommunications."[53] The commission also reflects on the post–Cold War security environment. Terrorism and crime and nonstate actors, rather than state-backed aggression, are the threats that receive attention.[54] Here, the PCCIP describes terrorism, financial crimes, and narcotics trafficking as the "dark side" of the new political, economic, and technological geography.[55] The report tentatively, and briefly, reckons with the economic and political foundations of infrastructure vulnerability. The commission acknowledges that deregulation made networks both more brittle and less accountable (it explicitly focuses on the regulatory changes in the energy, shipping, and telecommunications sectors).[56] Political restructuring, in its view, created efficient networks. But these changes carried a high price. The PCCIP writes that "today's processes are more efficient, but they lack the redundant characteristics that gave their predecessors more resilience."[57] That is, without the slack that used to be found within regulated infrastructures, even small attacks and disruptions can be amplified and have a significant impact.

In total, the commission painted a stark picture: the welding together of a global, just-in-time economy, defined by the ready movement of information, goods, and people, lowered the cost for terrorists and others to cause significant harm. The PCCIP offered modest recommendations—greater information sharing between the public and private sectors, the establishment of a new office of infrastructure assurance within the White House,

an increase in education and awareness around infrastructure threats and vulnerabilities, and more.[58]

The PCCIP's report landed with a thud. Like the reports that preceded it, it largely went unnoticed. One of the commissioners, Mary Culnan, a Georgetown professor, joked that if the authors of the report wanted to get their picture taken with the president, they would "have to go down to the White House and get one of those big cardboard cut-outs [to] pose with."[59] Efforts to brief the president and vice president on the commission's findings were not successful.[60] Commissioner Bill Harris of the Association of American Railroads was equally tart, wryly remarking that "we were invited once to a larger meeting where the President was a hundred feet away from us. … That's as close as we ever got. We were never invited to the White House. … I didn't feel that anybody at the White House really cared about what we were doing."[61] The commission wanted a strong public statement from the president about the importance of the topic.[62] Months later, President Clinton did eventually reference the PCCIP's work somewhat indirectly during remarks at Annapolis.[63] To PCCIP chairman Marsh, this was not nearly good enough. As he remarked: "You would think that after eighteen months full-time effort … it would warrant … some strong statements out of the bully pulpit. But it didn't."[64]

Despite the cool reception, some internal changes were afoot. On May 22, President Clinton signed a new Presidential Decision Directive (PPD) that followed up on the PCCIP's work. PPD 63—"Protecting America's Critical Infrastructure"—envisioned the protection of infrastructure as a short-term challenge.[65] The PPD stated that by 2003 the U.S. would have the ability to protect critical infrastructures from intentional attacks that might affect government services, public health and safety, or the orderly functioning of the economy.[66] PPD 63 defined critical infrastructure as "those physical and cyber-based systems essential to the minimal operations of the economy and government."[67] In language that would be adopted nearly word-for-word in the Patriot Act in a few short years, PPD 63 stated that it was U.S. policy that "any interruptions or manipulations of [critical infrastructure] must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."[68] PPD 63 moved with a light touch. Rather than pushing for the creation of new binding regulations on infrastructure operators, it supported voluntary cooperation between government and the private sector. It was explicit: critical infrastructure protection should be market-friendly. Close coordination between the public and private sectors is essential. After all, most infrastructures are owned and operated by

the private sector. Yet the PPD was clear that government should "to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector."[69] It went on to note that "incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection."[70] In cases in which market failure made some form of government intervention necessary, agencies should "identify and assess available alternatives to direct regulation," such as providing information for market participants and designing incentives.[71] The PPD called for the designation of a public-private National Infrastructure Assurance Council made up of private-sector infrastructure owners and operators and state and local officials. It placed a lead government agency in charge of each identified infrastructure and ordered the creation of the National Infrastructure Assurance Plan within 180 days. A new position within the White House, the national coordinator for Security, Infrastructure Protection, and Counter-Terrorism, was in charge of carrying out the new directive.

By the dawn of the presidency of George W. Bush, it looked like critical infrastructure protection would remain largely as it had throughout the Cold War and immediate post–Cold War period: a somewhat esoteric concern debated within a narrow circle of policy-makers and specialized researchers. By early 2001, the federal effort to protect critical infrastructure was led by the Critical Infrastructure Assurance Office—an obscure office hidden within the Department of Commerce's Export Administration with a modest annual budget of $5 million.[72] Total federal critical infrastructure spending fluctuated between $1.1 billion and $2.7 billion between 1998 and fiscal year 2001.[73] Before 9/11 the Bush administration had little appetite for investing in critical infrastructure protection, or homeland security, for that matter. A high-profile federal commission chartered in the late 1990s by Secretary of Defense William Cohen (and supported by President Clinton and Speaker Newt Gingrich) attempted to sound the alarm regarding terrorism and infrastructure vulnerability. Chaired by former Senators Gary Hart and Warren Rudman, the U.S. Commission on National Security/21st Century released its final report in February 2001, just days after the inauguration of President Bush.[74] The Hart-Rudman Commission conducted a detailed study of the post–Cold War national security environment. In one of its key recommendations, the Hart-Rudman Commission called for the creation of a new National Homeland Security Agency to oversee homeland security and, crucially, the protection of the nation's critical infrastructure.[75] In its view, infrastructure security was emerging to be one of the significant security

challenges of the 21st century, and the federal government did not have the capability in place to identify and address infrastructure vulnerabilities in a meaningful way. The Bush administration was skeptical of the idea of creating a new cabinet-level agency.[76] The Hart-Rudman report, like many others before it, was largely ignored. Chairman Rudman noted ruefully that the report went into the "dustbin at the White House."[77]

These scattered reports and commissions were attempts to invert infrastructure: to push to the foreground the systems that make up much of the background or our daily lives. In their own way, they each pleaded with policy-makers and, at times, the public to take note and look at the vulnerable foundations of contemporary life. They sought to plant infrastructures in the realm of security policy and view these systems through the lens of larger questions of geopolitics and conflict. By their own authors' ready admissions, these efforts largely failed. They rarely, if ever, sparked lasting or significant change. Yet threaded through these reports, documents, and marginalia is the creation of a way of understanding infrastructures that would later become powerful. Each of these reports and policy initiatives, in different ways, framed infrastructures as objects of anxiety and danger. They looked at different threats—a strike from the Soviets, terrorism, and other sources of possible attack and disruption. But they all agreed that the boring artifacts of modern life—electric power substations, wastewater plants, rail shipments, natural gas pipelines—were targets in waiting. They laid the groundwork for a cultural understanding of infrastructures as sites of danger in need of protection from external threats. The ideas charted through successive policy reports and mulled over for decades in the various odd corners of the federal government and aligned think tanks suddenly became in vogue in the post-9/11 context. After the terrorist attacks of 9/11, President Bush quickly adopted the vocabulary of the PCCIP: *critical infrastructure* found its way into speeches, executive action, legislation, and related press accounts with regularity. As President Bush pushed aside his earlier priorities and counterterrorism became central to U.S. policy, infrastructure security, or as it was now inevitably described, *critical infrastructure protection*, became a key pillar of this strategy. Moving forward, this conceptual framing and way of speaking and thinking about infrastructure would be taken for granted. The far-reaching and unanticipated consequences of this change would unfold in the coming years.

Institutionalizing Infrastructure Security: The Creation of the Department of Homeland Security

Infrastructure security became a top priority—at least symbolically—immediately after 9/11. But how *or if* this new prioritization would translate in practice was anybody's guess. During the first few months after 9/11, it was not at all clear if the repeated mentions by the administration of "critical infrastructure protection" were hollow or signaled the prospect of serious change. At first, it appeared that the Bush administration might balk at putting real muscle behind infrastructure security. The Patriot Act and the EO that established the Office of Homeland Security certainly borrowed concepts and ideas directly from the work of the PCCIP (and its predecessors). But the Patriot Act, as noted above, had only modest funding for new infrastructure security initiatives. While the Bush administration was quick to adopt the language and rhetoric of the PCCIP, how exactly it might approach the nuts and bolts of addressing infrastructure security was unclear. The PCCIP final report had pushed for the adoption of increased information sharing, a new White House office devoted to infrastructure security, and the creation of a private-sector council devoted to debating high-level issues. All of these modest recommendations had already been adopted in various forms by the late 1990s. The Hart-Rudman Commission outlined fairly grand ambitions. It called for the creation of a new cabinet-level homeland security agency tasked with infrastructure security as a key priority. The Bush administration resisted. It opposed creating a homeland security agency both before and in the months that followed 9/11.[78] In October 2001 Senator Joe Lieberman and Representative Mac Thornberry began to push a bipartisan plan to create a new "super agency" focused on homeland security.[79] Their plans would have merged a variety of agencies that had some homeland security responsibilities—something similar to what the Hart-Rudman Commission proposed—into a larger configuration. The White House rejected the idea. Throughout 2001 and into the late spring of 2002, the president and his aids repeatedly rejected the idea of creating a new homeland security agency. Instead, they supported the status quo.[80]

After beating back the idea of a new cabinet agency for months, in an about-face the president announced a proposal to create the new Department of Homeland Security during a televised address on June 6.[81] The reasons for the change in position are not entirely clear, but, as Mariano-Florentino Cuéllar argues, the decision to throw support behind a new agency likely reflected some mix of a recognition of the rising public

and congressional enthusiasm for reorganization and a concern over the upcoming midterm elections.[82] The president's plan was even more ambitious than the previous congressional proposals. It included moving parts of over 20 agencies into the new department, including many functions and responsibilities, such as trade enforcement and agricultural regulation, that did not obviously fit within the definition of homeland security.[83] Under the president's proposal, the new department would have four directorates, including one devoted to information analysis and critical infrastructure protection.[84] After sustained haggling with Congress, President Bush signed the Homeland Security Act of 2002 into law on November 25, 2002.[85] In remarks that accompanied the signing of the bill, President Bush stated that "the new department will analyze threats, will guard our borders and airports, protect our *critical infrastructure*, and coordinate the response of our nation for future emergencies."[86] It was a massive reorganization. The new Department of Homeland Security (DHS) would contain roughly 170,000 employees and transfer all or part of 22 agencies to DHS.[87] The department followed, in broad strokes, the president's initial proposal.[88] DHS was organized around four directorates: Border and Transportation Security, Information Analysis and Infrastructure Protection, Science and Technology for Homeland Security, and Emergency Preparedness and Response.[89] The department's core mission focused on preventing terrorist attacks, reducing the United States' vulnerability to terrorism, and minimizing the consequences of terrorism.[90] The act created an undersecretary of Information Analysis and Infrastructure Protection (IAIP) to lead the new directorate and added two assistant secretary positions within the directorate—an assistant secretary for Information Analysis and an assistant secretary for Infrastructure Security.[91] The IAIP was tasked with assessing the vulnerabilities of critical infrastructure and reviewing threats and mitigations.[92] The directorate was also directed to produce a comprehensive infrastructure security plan and help prioritize efforts by state and local governments, other federal departments, and the private sector.[93]

Infrastructure protection took a prominent role in DHS and across the federal government. An institutional transformation was unfolding. Indeed, as homeland security funding started to flow, the commitment to critical infrastructure protection became clear. Federal support for critical infrastructure protection grew quickly. In 2003 the IAIP directorate was funded at $177 million; by 2004, its budget ballooned to $824 million.[94] This was a far cry from the $5 million budget that had previously propped up the Critical Infrastructure Assurance Office within the Department of

Commerce back in 2000–2001. Federal support for critical infrastructure security would only continue to spike in the coming years. Through various reorganizations of DHS, infrastructure security would remain a consistent priority.[95] By 2016, DHS was receiving $5.6 billion annually to fund its critical infrastructure work.[96] Total federal spending on critical infrastructure security likewise grew sizably, from just over $2 billion in 2001 to a stunning $20.7 billion in fiscal year 2016.[97] By 2016, federal funding devoted to critical infrastructure protection accounted for roughly 30% of *all federal homeland security funding* (which totaled a staggering $71.7 billion).[98] With the creation of DHS, infrastructure security was now—and would remain—an unambiguous key governmental priority. It sat as a key element of DHS's new mission and organizational design. The largest reorganization of the federal government in over five decades—since the creation of the Department of Defense—hinged in part on the prioritization of infrastructure security as an important governmental responsibility.[99] It was a stunning transformation. By 2016, over two dozen federal departments, agencies, and offices would report significant spending on critical infrastructure protection.[100] For decades, little-read reports produced by the bushel had been trying to nudge infrastructure security onto the top of policy-makers' agendas and into the public's consciousness, with little success. As one participant in the PCCIP noted, the phrase *critical infrastructure* had seemed "tailor-made to evoke yawns."[101] This marginal set of ideas moved to the center of policy discussions and now federal funding. It was both cemented in the culture and concretized within an expanding web of new institutions devoted to critical infrastructure protection. The idea that infrastructures were insecure spaces in need of protection from external threats—that these familiar systems should be viewed through the lens of larger geostrategic security concerns—firmly took root.

The Politics of Risk: The Radical Possibilities of a Promiscuous Resource

The rise of infrastructure security as a topic of significant public concern set the stage for new debates and conflicts over how infrastructures should be organized. Now, the context of even routine discussions and decisions about infrastructure operation—decisions about where to build a new high-voltage electric power line, policies concerning how a small municipal water system should operate, and many others—was colored by larger concerns about terrorism and security.[102] This shift in context

created a crisis of control.[103] There was no simple road map indicating how to integrate security protections into the day-to-day operations of expansive, multiuser, multiuse networks. This moment of crisis created a space to rethink and to remake how infrastructures would operate. Over the next decade and counting, infrastructures would become deeply contested spaces. The wisdom and impact of deregulation would be revisited and questioned. Infrastructure owners, workers, different sets of users, civil society groups, government regulators, and others fought (and in some instances continue to fight) bitterly to define the terms upon which infrastructure protection would rest. Before mapping how these disputes played out within the postal system, freight rail transportation, and electric power grid, it is useful to pause and consider the politics of risk. To understand how organized interests would marshal the threat of terrorism to transform infrastructures—how the fear of terrorism would be translated into durable sets of new infrastructural practices—it is useful to first take a detour and consider the political possibilities and limits of risk.

Novel risks are volatile political resources: they can scramble the status quo in surprising—even contradictory—ways. In some cases, risks can provide the foundation for new forms of democratic activity and political formations. They can split open previously closed domains to close scrutiny and support new forms of collective action; they can rip topics seen as outside of politics back into public view and consideration; and, at the same time, they can offer the scaffolding upon which new political coalitions are created. In certain circumstances risks can spark political reversals: they can support the democratization of spaces previously cut off from public participation and accountability and amplify the voices of marginalized groups. But these are only possibilities—and fragile possibilities at that. As the coming pages and chapters detail, the politics of risk are complex. Risks can also be twisted to serve illiberal purposes, serving to squelch debate and reify existing concentrations of power. How, then, can we make sense of the promiscuous possibilities of risk as a political resource?

The work of Ulrich Beck provides a useful set of concepts to navigate the promise and pitfalls of the politics of risk. Beck sees that new risks have the possibility of enlivening democratic politics. His central thesis posits that society is entering a period of late modernity characterized by the centrality of new forms of risk. For Beck, new forms of risk now sit at the center of political debate. While traditional political conflicts within modernity centered, to a large degree, on the distribution of "goods," such as wealth and jobs, Beck now sees the distribution of "bads"—forms of harm and danger—as central. As he writes:

> With the advent of risk society, the distributional conflicts over "goods" (income, jobs, social security), which constituted the basic conflict of classical industrial society and led to attempted solutions in the relevant institutions, are covered over by the distributional conflicts over "bads." … They erupt over how the risks accompanying goods production … can be distributed, controlled, and legitimized.[104]

Beck argues that as part of this turn, society can now be conceived of as a *risk society*. The production of new forms of risk, defined in keeping with the term's colloquial meaning as forms of harm and danger, are internal to the process of modernization—they are what Anthony Giddens refers to (in an unintended echo of the PCCIP's similar language) as the "dark side of modernization."[105] The production of risks is not a failure of modernization but rather a side effect. As Beck notes, "In advanced modernity the social production of *wealth* is systematically accompanied by the social production of *risks*."[106] The management of these sorts of risks is now a central feature and challenge of contemporary life.[107]

It is a provocative idea. For Beck, these risks are politically explosive. They have the potential to create institutional turmoil and disruption. Although forms of harm have, of course, always existed, a new category of risks—climate change, terrorism, systemic infrastructure failure, among others—are different. They are expansive—unmoored in time and space—global in scope, potentially catastrophic, and resistant to calculation.[108] These types of risk cannot be reduced to a specific location or fixed temporal period: to whom and where these harms might strike is not clear. Precisely *whose* problem such risks are is an open question.[109] Nor can they be reduced to easy estimates of frequency or degree of danger: they outrun our ability to tabulate either their likely occurrence or severity with great confidence.[110] These risks are atypical, infrequently occurring, and quite new, making historical extrapolation difficult.[111] As a result, uncontested statements about the danger they present are hard to offer. Calculability is central to the management of risks by supporting empirical testing and the provision of mitigation measures, including insurance. Absent accepted measures of probability, central institutions involved in managing risks—namely, branches of science, political bodies, and insurance—are destabilized.[112] In this manner, risks such as those associated with ecological collapse, nuclear waste, and terrorism, to select three risks Beck regularly invokes, undermine and challenge the ability of existing institutions. They create a crisis of legitimacy and a crisis of control.[113] Now, everything seems contestable and open to renegotiation.

New forms of risk hold out the possibility of radical change.[114] For a moment, as Beck writes, "The unthinkable and unmakeable become

possibilities."[115] The democratizing potential of risk operates across two distinct, though related, trajectories. On the one hand, risks can open previously closed domains and illuminate the political choices and implications buried beneath the surface.[116] The recognition of risks can draw attention to the political implications of seemingly private and apolitical areas and, in the process, can create openings for new political engagements at odds with the status quo.[117] Areas typically considered private and apolitical, such as business, economics, and science, are now politicized and subject to public scrutiny and discussion; they become legitimate topics of political discussion and intervention. As Beck notes, the recognition of new forms of risk can lead

> previously depoliticised fields of decision-making [to become] politicized.… Generally involuntarily and against the resistance of … powerful institutions … they are opening up these problems to public doubt and debates. In global risk society, therefore, subjects and themes once treated behind closed doors, such as public investment decisions, the chemical composition of products and medicines, scientific research programs and the development of new technologies, are articulated and debated in public.[118]

The recognition of the production of risks within areas considered private and "off-limits" illuminates the inherent politics at play. In doing so, it offers the possibility of opening these areas for participatory politics and some form of collective control. At the same time, risks also function as a resource for otherwise marginalized groups to enter into political discussions and coalitions. The recognition of novel risks enables new actors to enter the fray. The uncertainty surrounding the probability and effects of novel risks creates a space where new types of claims can be offered and taken seriously, and new sets of speakers can find a voice. New risks expand the horizon of possibilities and enable "as if" thinking. Once risks are publicly accepted and salient, a range of imagined possible scenarios are credible; as Beck notes, the subjunctive replaces the indicative mood.[119] In other words, novel risks enable a new type of thinking structured around the hypothetical or possible. If the past no longer is taken to offer a clear image of the future—if the future is no longer presumed to mimic the past—the limits of what is considered plausible are stretched. Claims and scenarios of what *could* happen are taken as legitimate. In this moment, new and existing social movements can adopt risks as a clarion call that challenges the accepted wisdom of the status quo and, importantly, challenges power.[120] The production of new risks creates seams where challenges to the authority and legitimacy of those in power are possible.[121] As Beck argues, "The boundaries between scientific

and unscientific, between science and politics, and between experts and layman" erode.[122] Here, monopolies of knowledge are challenged and expert claims become contestable. This creates a space for new possibilities. Now a range of voices, including actors not typically authorized to speak with authority, are able to enter substantive debates.[123] In this respect, risks serve as a type of capital that is not reducible to existing political, economic, or scientific power.[124]

This optimistic portrait of risks must, however, be qualified. The political possibilities of risk are fragile and contingent. Risks are not inherently transformative; they offer the potential for political transformation. They are a resource open to appropriation, a source of legitimation and external support that actors of different stripes can highlight and rely on in advancing their positions. Risks are unreliable allies to power because their definition and interpretation do not necessarily follow established currents of power.[125] The potential of risks, for Beck, is the gap between what he terms *relations of definition* and other forms of power.[126] It is in this disjunction, between who defines risks and existing forms of power, that the radical potential of risks rests.[127] But what direction transformations linked to the recognition of novel risks will take—in support of democratization or the retrenchment of power; in favor of wise reconsideration or the headless rush of paranoia—is always an open question. The political potential of risks is simply that: *potential*. It requires organized interests to adopt risks and advocate for change.

Political, economic, and technological changes are creating new forms of peril that have real consequences and stakes. Yet, critically, these risks are always open to interpretation and mediation. That is, what risks mean and how they are thematized and translated into new policies and procedures is an open question. Risks do not in and of themselves compel action in particular directions; they can be used as symbolic resources for quite different ends.[128] The invocation of novel risks can support a reflexive democratic politics that considers the sources of new forms of danger and new courses of action or, alternatively, a type of totalitarianism that impoverishes participation in the name of emergency measures.[129] Democratization and contestability are useful and important correctives to the fencing off of political questions. But there are real and significant challenges that cannot be overlooked. If everything becomes open to questioning, then paranoia, conspiracy theories, and antiscientific crusades are also given room to flourish. In exploring the politics of risk, a set of key questions now slide into view: How, by whom, and to what end are risks interpreted and marshaled as a resource?[130] How have the

exceptional circumstances of novel risk been fashioned into a durable set of security practices? And, most crucially, what social relations are embedded within new security practices? These questions provide useful guardrails for examining and understanding the implications of the new forms of infrastructure security that will transform the postal system, freight rail network, and electric power grid in the coming years.

Beck leaves us with a useful starting point: the ultimate significance of risks requires investigation into how groups mobilize around and deploy the symbolic currency or capital embodied within new risks. Once risks become relevant and salient—accepted as legitimate points of reference within the stock of common images, meanings, and arguments that define a shared culture—they can be adopted and wrenched to support new claims.[131] As certain risks are accepted as legitimate within the larger common culture, they can be appropriated by diverse sets of actors to justify action. In pointing out this dynamic, Beck is making a clear connection between two different understandings of culture—between viewing culture as a shared set of common, but by no means static or uncontradictory, meanings and culture as a repertoire of available tools. In this reading culture is shared, interpersonal, and collective: it is a broader structure within which action makes sense and is intelligible. In this fashion, Beck forwards a notion of culture that is compatible with Clifford Geertz's interpretive notion of culture as a shared semiotic framework or context within which action can be described.[132] Yet in identifying how cultural notions of risk can be instrumentalized as resources of legitimation, Beck shares an affinity with Ann Swidler (and others) in emphasizing how the broader set of available meanings within a culture enables and supports autonomy. In her well-worn phrase, culture acts as a "tool kit," a repertoire of available ideas from which individuals can draw to support actions. As Beck argues, risks empower marginalized groups because they offer "new sources of legitimation"—a new tool in the tool kit.[133] Risks "provid[e] political movements with the external conditions, strategies and resources for a type of 'judo' politics. That is to say … [risks] unleash powerful impulses for change from positions of relative powerlessness."[134] Here, culture does not compel action and is not deterministic or oppressive in a functionalist mode. On the contrary, it enables autonomy. It is through the availability of cultural resources that "strategies of action" can be forged.[135]

This view of the politics of risk is striking. It is at odds with how risk is usually thought to function within political life, particularly in the realm of national security policy and certainly in the context of post-9/11

security interventions. It is often taken as a given that new risks, emergencies, and security interventions lead to the suspension of democratic processes. In moments of peril, it is said that the powerful are uniquely positioned to seize power. This view abounds. The concept of *securitization*, developed most centrally within security studies by Barry Buzan, Ole Waever, and Jaap de Wilde, suggests that security is, primarily, a rhetorical device used to justify exceptionality in support of the powerful.[136] Studies of securitization see "security" as a trump card used by the state to suspend the regular features of governing and seize power. As Buzan and colleagues note: "'Security' is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics."[137] In this thinking, security necessarily blunts normal democratic mechanisms. As Buzan and coauthors remark:

> Securitization … means to present an issue as urgent and existential, as so important that it should not be exposed to the normal haggling of politics but should be dealt with decisively by top leadership prior to other issues. … It works to silence opposition and has given power holders many opportunities to exploit threats for domestic purposes, to claim the right to handle something with less democratic control and constraint.[138]

This notion of the politics of risk—as something inherently antidemocratic—has been widely adopted by observers of the post-9/11 moment. In *Fear: History of a Political Idea*, Corey Robin critiques at length the notion that fear and risks—particularly the risk of terrorism post-9/11—can serve as the foundation for democratic revitalization and engagement.[139] For Robin, risks are the exclusive province of the powerful; anxiety, fear, and uncertainty only support greater concentrations of power and are put in service to reduce public participation and freedom.[140] In Robin's reading, risks obscure the political character of situations and justify the suspension of normal democratic processes in response to the needs of a presumed emergency. John Mueller in *Overblown* offers much the same argument in reference to post-9/11 politics, and certainly, many examples of how risks have been used to justify exceptionality at the expense of democracy can be offered.[141] But these accounts adopt either implicitly or explicitly a somewhat limited notion of culture. In these, iterations culture is little more than the scrim through which the powerful impose their prerogatives. This view is blinkered. Culture is more than the distillation of the ideas and notions the powerful hope to promote. Culture is rich and messy: it contains contradictory ideas and arguments. It is, following James Carey's discussion of a cultural approach to communication, a shared set of meanings that provide the larger context within which ideas

and arguments make sense.[142] Once risks are publicly salient—once they have moved from being on the edge of legitimate discourse and are more or less taken to be true and have taken up residence as part of the larger shared culture—they are no longer the province of a particular speaker. In these moments, the stakes are high. Both the powerful and the marginalized can fight to appropriate the language of risk for their own ends. The powerful can claim that exceptional circumstances require setting aside democratic norms and processes. They can (and often do) cloak their agenda in the language of risk and use it as a means to accumulate or consolidate power. But those outside of power can also enact securitization—they can speak the language of security and exceptionality as a way of challenging the existing status quo. Securitization can work not only to silence but to amplify voices. The exploitation of threats can be put into the service of democratic participation. Risk, in and of itself, does not compel a particular outcome. What is left then is a demand for close examination how risks circulate and are deployed. This is precisely the task to which the following chapters turn. After 9/11 the cultural reframing of infrastructures as dangerous things and the creation of institutions that supported this view were firmly put in place. These changes set the stage for a significant transformation: a possible reordering of the material outlines and power dynamics that defined infrastructure. How this transformation would unfold, however, was an open question.

Infrastructure Inversion and the Politics of Post-9/11 Security

After the attacks of September 11, infrastructures were recast as sites of vulnerability, danger, and fear. This reordering was driven by clear choices—specifically the decision of the Bush administration to adopt the PCCIP's (and other earlier groups') framing of infrastructures as sites of danger and the subsequent decision to make infrastructure protection a clear, and well-funded, government priority within DHS and across the federal government. The difficulty in calculating the risk of terrorism became an acute problem; the possibility, rather than the probability, of catastrophic loss became a source of concern for the state, operators, and a host of publics associated with these networks. This was a rich moment. The political possibilities of risk described by Beck came alive. As infrastructures were revisited or redefined as sites of anxiety and danger—targets in waiting—they suddenly became open to reconsideration and remaking. The sunk politics of infrastructure, at least for a moment, would become visible; the upheavals of deregulation would reemerge as public

problems. The cultural and institutional reframing of infrastructures as dangerous objects created a crisis of control: it opened infrastructures up to competing claims about how they should be organized; it created an opportunity for otherwise marginalized voices to be heard; and it created an opportunity for new, surprising political coalitions to crystallize. It created real possibilities for change—possibilities that were not anticipated during the initial rush to include infrastructure protection within an expanding portfolio of homeland security during the early years of the Bush administration. During these early post-9/11 days, much remained unclear. How and on what terms would infrastructure security unfold? Who would define the contours of these new security measures? How would new, enhanced forms of security square with the needs of access, low cost, and reliability (among other values)? Importantly, what type of social relations would these new security interventions codify? Infrastructures are a nest of technical and nontechnical elements; they join together technical artifacts, legal standards and regulations, infrastructure owners, different sets of users and customers, and labor in a contingent set of relationships. How would new security interventions reorganize these relationships? In short, how would infrastructures order?

The answers to these questions would only gradually become clear in time. During the Bush and then Obama administrations (and as of this writing, the Trump administration), critical infrastructure protection would remain a key priority and point of fierce debate. The following three chapters explore in detail how new security concerns upended and eventually remade the postal system, the freight rail network, and the electric power system. They trace the *bureaucratization of risk*: how the abstract threat of terrorism—the idea of a possible terrorist attack at some point in the future—is written into stable and routine security practices, regulations, codes, and technologies. This process was contradictory. It led to both the opening of sealed domains and a type of democratic revitalization that challenged the changes unleashed through deregulation, and it also led to the further consolidation of power to control infrastructure. Indeed, in time both the promise and fragility of the politics of risk would become clear.