Letters, Power Lines, and Other Dangerous Things

The Politics of Infrastructure Security

OA Funding Provided By:

The open access edition of this book was made possible by generous funding from Arcadia—a charitable fund of Lisbet Rausing and Peter Baldwin.

The title-level DOI for this work is:

doi:10.7551/mitpress/10541.001.0001

Introduction

Letters, Power Lines, and Other Dangerous Things

On March 12, 2013, Director of National Intelligence (DNI) James Clapper publicly testified before the Senate Select Committee on Intelligence.[1] As DNI, Clapper sat atop the U.S. intelligence bureaucracy, coordinating and overseeing the efforts of 17 different intelligence agencies, bureaus, offices, and services, including the National Security Agency (NSA) and the Central Intelligence Agency (CIA). Clapper was plainly uncomfortable. A long-standing veteran of the intelligence world, Clapper could not help but note that "an open hearing on intelligence matters is something of a contradiction in terms."[2] Reading stiffly from prepared remarks, Clapper presented the 2013 *World Wide Threat Assessment*, an annual unclassified summary of the intelligence community's consensus assessment of threats to U.S. national security.[3] In an unprecedented and important symbolic move, the intelligence community listed threats—specifically cyber threats—to critical infrastructure networks first.[4] Threats targeting critical infrastructure ranked ahead of weapons of mass destruction, terrorism, and transnational crime.[5] The assessment revealed, in Clapper's words, "how quickly and radically our world—and our threat environment—are changing."[6] The nation's top spy might question the wisdom of public testimony, but he was nonetheless clear: infrastructure protection was emerging as *the* challenge of the 21st century.

Clapper's prioritization of the protection of critical infrastructure—systems that include telecommunications networks, the electric power grid, financial systems, transportation networks, and others that the federal government views as essential to the nation's security, health, and economic prosperity—is the culmination of a transformation in how policymakers and much of the public view infrastructures. In the years since the terrorist attacks of September 11, 2001, infrastructures have been recast as sites of anxiety and danger. The mundane systems that undergird much of modern life acquired a sinister tint: no longer were these networks simply regarded as the boring background wiring of modern society; they were now *soft targets* that immediately required new, enhanced protections. In the weeks and months that followed 9/11, President George W. Bush made it clear that infrastructure security would be a key plank in a new, expansive homeland security agenda. In quick succession, a patchwork of new laws, policies, technologies, and practices focusing on infrastructure protection unspooled. In October 2001, Bush created the Office of Homeland Security within the executive branch and tasked it with coordinating federal infrastructure protection efforts. The Office of Homeland Security would, in a matter of mere months, be replaced by a vast newly created federal department: the Department of Homeland Security (DHS). The creation of DHS was a massive reorganization—the largest reshuffling of the federal government since the establishment of the Department of Defense in 1947.[7] Infrastructure protection sat at the center of DHS's new mandate. The primacy of infrastructure protection endured during the administration of President Obama and has showed no signs of waning during the Trump administration.[8]

The reframing of infrastructures as insecure spaces justified a significant and unprecedented investment in infrastructure security. It was a stunning transformation. For years a string of public commissions, policy reports, and little-read think-tank missives had warned that the nation's infrastructures were vulnerable to attack. Before 9/11 they tried, again and again, to push policy-makers and the public to prioritize infrastructure protection. Their warnings went largely ignored. In early 2001 the federal effort to protect critical infrastructure was being run from the Department of Commerce's Bureau of Export Administration by a tiny, obscure office—the Critical Infrastructure Assurance Office—with a modest annual budget of $5 million.[9] Across the entire federal government, critical infrastructure protection spending ranged from $1.1 billion to $2.7 billion annually between 1998 and fiscal year 2001.[10] Infrastructure protection was, at best, little more than an afterthought. Two decades later, the picture is radically different. Infrastructure protection is now a priority. By 2016 the federal government would devote a staggering sum—over $20 *billion*— to critical infrastructure protection annually.[11] DHS alone now receives over $5 billion annually to fund programs directly related to infrastructure protection. Across the federal government, roughly one-third of all homeland security spending is devoted to infrastructure protection.[12] If anything, these numbers significantly underreport government spending on infrastructure protection. They do not include state and local efforts, private-sector investment, or border and transportation security—a distinct federal funding category currently divorced from critical infrastructure protection in public accounting. If border and transportation security are added to the mix, the figures begin to overwhelm: $51.5 billion in total federal funds—70% of federal homeland security funding—is devoted to protecting the nation's infrastructure.[13]

The influx of funding and attention has left its mark. The post-9/11 emphasis on infrastructure protection has remade the material and organizational foundations of infrastructures. Some of these new interventions are obvious and hard to miss. Barricades, bollards, and large, ugly concrete "security planters"—oversized flowerpots designed to thwart cars and vans from ramming into buildings, mowing down pedestrians, or delivering a deadly explosion—dot busy city streets and public squares.[14] Boarding a commercial flight heading from Boston to San Francisco now requires a familiar post-9/11 ritual: shoes, belt, and coat slipped off; shampoo, conditioner, and all other liquids stored in clear ziplock bags; laptop removed from the backpack and placed (always alone, never with shoes or coat) in a plastic bin for x-ray; arms raised as you stand inside an advanced imaging technology (AIT) body scanner for inspection; and then waiting until the Transportation Security Administration (TSA) agent tells you to collect your things and continue on your way, a few steps closer to your flight and to San Francisco.[15] Symbols of post-9/11 infrastructure anxiety are everywhere. Posters and signs plastered in train stations and subways running underneath New York City proclaim what the *Washington Post* describes as the nation's unofficial motto of post-9/11 life: *If you see something, say something*.[16] Dreamed up by a New York advertising executive on September 12, 2001, the slogan has become a marker of a transformed landscape: riding subways and trains now requires constant vigilance. Infrastructures are not just the foundations of contemporary life: they are fragile targets in waiting.[17]

Other infrastructural changes and alterations are subtle and can be difficult to see. Inside post offices across the U.S., detection and tracking systems developed by the defense contractor Northrop Grumman now test millions of letters for hints of a possible biological attack as they whirl through the postal network each day.[18] New security practices reach deep into the "guts" of infrastructure. Verizon, AT&T, and other commercial Internet service providers (ISPs) use classified information provided by DHS to scan data flowing over their commercial networks for signs of malicious traffic.[19] New security regulations require workers at the nation's ports to submit fingerprints and undergo a "security threat assessment" in order to receive a Transportation Worker Identification

Credential (TWIC) from the TSA before accessing ports and vessels.[20] These changes may not be obvious to the public. For those of us outside of these infrastructures, they can be easy to miss. But, they matter: new security practices are remaking infrastructures in ways that will endure for decades (or longer). These changes may first be introduced during a moment of fresh panic, but once in place they become encased in custom and habit. In time, what was novel becomes simply "the way things are done": security practices become entrenched as part of the sunk politics of infrastructure that is taken for granted as normal and dull.

Behind the web of new security policies, laws, and embedded technologies that oversee infrastructure sits a larger long-running battle over infrastructural control. Infrastructures are systems that support *other* forms of activity. When they work well, we hardly notice them. As Paul Edwards observes, these systems become taken for granted, part of the "naturalized background, as ordinary and unremarkable as trees, daylight, and dirt."[21] Infrastructures are, to be sure, platforms. They are the foundations upon which other forms of activity rest. But they are not, nor have they ever been, *neutral* platforms.[22] The terms upon which they operate matter: infrastructures organize users, owners, regulators, workers, and uses in particular relationships that benefit and recognize some at the expense of others. From the moment they are created until the moment they are discarded, abandoned, and left to rot, infrastructures are sites of conflict over the terms of these relationships. These skirmishes often occur mostly offstage, buried within technical reports, arcane debates about cost allocation methodologies, and little-attended public hearings on zoning ordinances. Occasionally, however, infrastructures are inverted: the systems that sit in the background are briefly thrust into the foreground. These are key moments. For a fleeting instant, infrastructures are made visible and open to significant change. The political choices—power—inscribed within their operation become bald. The aftermath of 9/11 was one such moment. Infrastructures were now suddenly visible and open to renegotiation. The stakes were high. The administration of President George W. Bush might have made infrastructure protection a priority, but it left much of the details about how these vast networks and systems would actually be secured or protected unclear—the details would be worked out in the years to come. A cross section of actors and coalitions clashed and fought for control. New forms of security held out the real possibility of reshuffling how infrastructures are organized: Which sorts of users would be favored under new security guidelines? What type of uses would be deemed risky? Who would have a voice in crafting new security protocols—workers, local politicians, industry? New security practices threatened to scramble how infrastructures operate and are organized; they held the potential to upend these sociotechnical systems in ways that might intensify or reverse the currents of power and control for years to come. In making sense of new forms of security, then, it is important to ask not only whether new security practices "work" but also "For whom do they work?" and "What type of social relations do they produce?"[23] These and other questions hung in the air during the first two decades of the 21st century as protecting infrastructure moved from being an idle and somewhat esoteric concern to an imperative.

* * * *

Letters, Power Lines, and Other Dangerous Things tries to make sense of the disorienting and contradictory infrastructural changes that have unfolded since September 11. It uncovers how the threat of terrorism is etched into the inner workings of infrastructures through new laws, regulations, technologies, and practices. The book maps these changes—why they happened, why they matter, and how they fit into the larger mosaic of both infrastructure governance and post-9/11 politics—through an examination of three U.S. infrastructures: the postal system, the freight rail network, and the electric power system. Each of these infrastructures underwent significant post-9/11 security overhauls. Cracking open the "black box" of infrastructure security practices reveals pointed conflicts, constitutive choices, and the accumulation of crosscutting forces that otherwise remain out of view. Rich and important stories emerge. Behind new forms of postal security sits a pitched, decades-long battle among unionized postal workers, key large-volume mailers, and postal management for control of the postal bureaucracy. Debates about how to protect against biological hazards—namely, anthrax—sent through the mail spiraled into larger arguments about the balance between workers' rights, the power of commercial, so-called junk mailers, and the shifting fortunes of old media in a new media world. New post-9/11 controls over rail shipments of toxic materials reveal how the rise of the "war on terror" enabled environmental activists to build a powerful coalition of activists, city and state officials, and members of Congress to take on the rail industry and the influential chemical lobby. A close look at the history of the first mandatory cybersecurity standards for the electric power industry illuminates how otherwise marginal federal regulators maneuvered to transform what appeared to be thin administrative powers into a robust system of accountability. These and other stories are written in the new security standards, regulations, and technologies embroidered within these larger networks.

This book casts post-9/11 infrastructure security efforts in a new light. It finds within contemporary infrastructure security practices attempts to create new forms of *public accountability*. In the three cases examined, new security interventions made or sought to make infrastructures open to the concerns and interests of different groups—*infrastructure publics*—that are defined through their connection to the larger system.[24] This opening, and attempted opening, of infrastructures to plural publics and competing logics was significant. In the decades before 9/11, political and economic restructuring pushed infrastructure governance increasingly out of the public's reach. Years of market-based restructuring elevated infrastructure owners and operators—and some particular customers—into positions of unrivaled power. These same changes in political economy also altered the material organization of these systems in ways that made them increasingly vulnerable to large-scale failures. In the three cases examined, post-9/11 reforms attempted to wrestle back public control and address the vulnerabilities that now pocked these systems. In an odd twist, the vernacular of the war on terrorism offered otherwise marginalized groups the opportunity to have their voices heard and supported the creation of new political coalitions that agitated for greater public supervision over infrastructure. The threat of terrorism was a useful and powerful political resource. New forms of infrastructure security attempted to address the vulnerabilities caused by market-based reforms and, at the same time, reassert a degree of public control—control characterized by a recognition of the different publics and values present—over infrastructure. These efforts were not always successful—postal reforms initially held out the promise of offering postal workers a greater stake in making major decisions about how the postal network would operate and evolve, but these hopes were short-lived as key players (large-volume commercial mailers) outmaneuvered the postal unions and reasserted and strengthened their grip on postal policy. But in both electric power and freight rail, concerns over terrorism and security provided the foundation for new, durable forms of public accountability.

This portrait complicates conventional accounts of post-9/11 infrastructure security. Critical appraisals of post-9/11 infrastructure security typically paint a decidedly bleak picture. Often, infrastructure security is seen as little more than "security theater": ritual displays that do little to actually enhance security while, at best, offering some psychological benefits.[25] Asking passengers to take off their shoes before boarding an airplane might do little to improve security, the thinking goes, but this bit of theater might make passengers feel safer. Elsewhere, contemporary infrastructure security efforts are taken to be a pretext for the troubling consolidation of power.[26] In this view, infrastructure security looks like an unholy alliance between corporate players and the state—what the author Naomi Klein describes as *disaster capitalism*. In this telling, rich and powerful groups use the exigencies of emergency and collective trauma to push through programs that line their pockets and extend their power at the expense of the less fortunate.[27] To be clear: these interpretations have value. But neither view—infrastructure security as pure theater or infrastructure security as corporate/state power gone rogue—is capacious enough to capture the complex and contradictory changes that have been enacted under the banner of infrastructure security. The cases assembled in this book point to a set of alternate and competing changes: *infrastructure security as public accountability*. Groups that traditionally sit outside of geostrategic security conversations were able to use the threat of terrorism to serve their ends. Greenpeace, the National Association of Letter Carriers, city councilors, and others rarely thought to be key players in the world of national security strategy were able to adopt and deploy the vernacular of the war on terror to carve out a space for expanded public participation in infrastructure. The threat of terrorism offered a potent resource to challenge the infrastructural status quo and, in some instances, enact meaningful change. The politics of security rarely unfold along a straight or predictable path. On the contrary, they include surprising reversals, contradictory changes, and, at times, utterly predictable moves. Ultimately, as the following chapters will make clear, the risk of terrorism circulates and is encoded within infrastructure in surprising ways, both reinforcing and challenging the status quo and alternately comforting and confounding power.

Letters, Power Lines, and Other Dangerous Things develops two key arguments—one a revisionist account of infrastructure history that underscores the political and economic origins of contemporary infrastructure vulnerabilities; the other a rethinking of post-9/11 politics that emphasizes the ways in which fears over terrorism and security were used to justify and enliven (with varying degrees of success) public accountability of infrastructure. These two threads knot together to tell an important story that challenges familiar narratives about the politics of risk and security and forges a revisionist account of the recent political and economic history of infrastructure: it underlines the ways in which fears over terrorism generated new forms of public accountability; it reframes security interventions as attempts to grapple with the legacy of decades of political and economic restructuring in favor of the market; and it offers a pointed reminder that the politics of risk are promiscuous, offering comfort and resources both for the powerful and the marginalized.

The Political Origins of Infrastructure Vulnerability: Regulation and Deregulation Revisited

Our story starts well before the morning of September 11, 2001. To fully grasp the pitched battles soon to be waged over new security practices—the stakes, the key players and coalitions, the surprising reversals, and the stubborn continuities across historical periods—it is important to begin by mapping the larger political and economic history of these networks. This is not just spelunking through history for its own sake and pleasure. Post-9/11 infrastructure changes are in large part attempts to reckon with the legacy and consequences of the political and economic restructuring of infrastructure that occurred during the last three decades of the 20th century. These changes—*deregulation*—set the stage for the post-9/11 transformations that would later unfold in two important ways. First, policies of deregulation worked to create new forms of infrastructure vulnerability. These vulnerabilities would in time become acute sources of political anxiety and, eventually, significant intervention after 9/11. Second, deregulation did more than simply transform the material outlines of how the postal system, freight rail, and electric power operated. The remaking of the political economy of infrastructure was, above all, a political project.[28] It transferred control away from public institutions and their associated norms of accountability in favor of key market participants. This change—the remaking of power within each infrastructure sector—would provide an important context for the later conflicts that would be fought in the early 21st century over how to secure and protect infrastructure.

Deregulation remade the postal, freight rail, and electric power systems. Beginning in the 1970s, the political economy of infrastructure in the U.S. (and across the globe) underwent a seismic change. Infrastructures were deregulated: long-standing public controls that supervised a range of sectors, including communication, transportation, energy, and other infrastructures, were relaxed or rescinded in favor of the market. The wisdom of the market would, the thinking went, substitute for public supervision and stewardship. As Tony Judt observes, the narrow language of economics would now become the principle vocabulary of public policy.[29] The dynamics played out differently in the postal system, freight rail, and electric power, but in each case, deregulation led to a reorganization in both how these infrastructures were managed and in the material contours of these networks. These political and economic changes delivered some real and presumed benefits. In some instances services became cheaper and more efficient, delayed capital improvements were finally realized, and inefficient practices could finally be cut. If nothing else, deregulation pushed infrastructures to become lean and efficient as never before: thousands of miles of freight rail track were abandoned as rail operations were consolidated in the wake of regulatory reform; freed from increasingly arcane methods of budgeting, the postal system moved to replace manual labor with new automated systems for processing the mail; the electric power system responded to deregulation by slashing investment in so-called gold plating (excessively priced equipment and services that were attractive under rate-of-return regulation) and began adopting standard off-the-shelf technologies.

But efficiency came at a price. There were negative costs for workers, particular users, and, ultimately, for infrastructure security. Restructuring pushed infrastructures into increasingly combustible formations. Deregulation led infrastructure owners and providers to adopt what Charles Perrow describes as tight-coupled and complex operational profiles—key changes that placed these systems on vulnerable footing.[30] In each system these changes made new types of large-scale failure possible or more likely. In time, after 9/11, these vulnerabilities would transform into salient political problems. But deregulation did more than interject new types of vulnerabilities into infrastructure systems. It also altered the broad dynamics of power that attended these systems. The rush to embrace the market limited public supervision and control over infrastructure, leaving key market players with significant leverage and the power to define and determine how these services would operate, while workers, environmental groups, local communities, and others with a stake in how infrastructures were organized saw their opportunities to shape these infrastructures comparatively narrowed. The old regulatory model, warts and all, at least held out the possibility of blunting market power with some acknowledgment of larger substantive concerns. Now, market power trumped other concerns.

Understanding this larger historical narrative is important. It demonstrates that the vulnerabilities that became public problems after 9/11 were not ahistorical inevitabilities: they sprang directly and indirectly from a set of concrete political and economic choices. The costs of security, then, can be seen as a long-overdue bill—they are in part the unpaid tab of deregulation. Contextualizing contemporary security interventions within this larger historical narrative offers an ironic and wry observation: the ostensible removal of infrastructures from government control in favor of the free hand of the market eventually winds up requiring billions of dollars annually in additional government spending and close, continual government monitoring and controls to make these systems stable. Beneath the continued functioning of liberalized infrastructures sit new risks, massive public expenditures, and increasingly intense governmental efforts to mitigate the newly constructed possibilities of failure.

At the same time, sorting through the twists and turns of deregulation is indispensable for understanding the context and significance of post-9/11 debates over infrastructure security. These debates were never simply about security—they spoke to larger concerns over power and infrastructural control. Drawing the larger historical picture makes this point plain. Fractious debates over who would pay for the added costs of postal security after the 2001 anthrax attacks, fights over the routes that trains carrying toxic material would take, and battles pitting bureaucrats inside the federal government against electric power companies over the proper definitions of critical cyber assets were always about something larger. They were about renegotiating the power to control infrastructure; they were attempts to claw back some measure of public accountability that had been lost through decades of political and economic reform.

Finally, linking these seemingly distinct historical moments—deregulation and later post-9/11 security efforts—highlights the interplay between political economy, the materiality of infrastructure, and risk. As international security scholar Claudia Aradau perceptively notes, critical accounts of infrastructure security often overlook the materiality of infrastructure, reducing these systems to mere "empty discursive receptacles."[31] Indeed, there is a hazard in viewing contemporary debates over infrastructure security too narrowly and treating these systems as neutral or absent objects. This view renders infrastructures as blank canvases upon which contemporary fears about terrorism are projected. Doing so leaches these systems of their history, materiality, and power. It runs the risk of ignoring the agency or power invested in the built world. The materiality of these systems matters. Systems organized in different ways encourage and enable certain types of uses over others—and they encourage and enable different possibilities of failure. Power is inscribed, reflected, and ultimately reproduced within the material organization of infrastructure. Focusing on the connections between deregulation and post-9/11 infrastructure security emphasizes how history and power are invested in the material configurations of infrastructure. This is not to say that risks are exclusively material—far from it. The identification, prioritization, and eventual interpretation of particular risks is a deeply social endeavor (as will be discussed in detail below). But, these discursive processes are entangled with the built world. The transformation of infrastructures into dangerous objects—into security problems—is jointly produced through a set of interlocking material and discursive changes.

Ubiquitous Targets: Infrastructure Security after September 11

In the wake of the terrorist attacks of September 11, infrastructure protection and security became a key priority. Now, seen through the exigencies of the expanding global war on terror, infrastructures were quickly transformed in the public imagination into "dangerous things," volatile formations that needed taming and control. Deregulation directly and indirectly went on trial. Decades of political and economic reform created systems prone to fail in spectacular fashion while systematically weakening public controls over these systems. Deregulation's relentless pursuit of efficiency above all else now appeared to be a bad bargain. The political and cultural realignment that occurred after 9/11 made these vulnerabilities legible and salient in a new way. This recasting of infrastructure as dangerous things ultimately led to contradictory changes. New security practices in some instances sealed off infrastructure from public debate and intensified controls targeting workers, users, and suspect network flows. These drastic measures were taken in the name of security. But this is only part of the story. As the second main thread of the book makes clear, novel security practices also led, with varying degrees of success, to new practices of public accountability. A range of groups that traditionally sit outside of discussions of geostrategic security adopted the language of the war on terror to carve out new spaces for public participation and oversight. These practices countered or contested the changes that occurred through decades of political and economic restructuring and opened infrastructures to diverse publics and democratized infrastructure.

The standard account of post-9/11 politics plots a troubling narrative. In this familiar telling, fear, uncertainty, and dread are employed by the state to promote the powerful and justify the diminution of a range of vital civil rights and democratic norms.[32] Mark Danner, writing in the *New York Review of Books* on the occasion of the 10-year anniversary of September 11, offered a sobering appraisal of the politics of the past decade and ventured a worried glance to the future.[33] Danner summarizes the time since September 11, 2001, as

> these years during which, in the name of security, some of our accustomed rights and freedoms are circumscribed or set aside the years during which we live *in a different time*. This different time has now extended ten years—with little sense of an ending.[34]

Danner's appraisal depicts post-9/11 politics as a period of profound and ongoing loss: a period during which cherished values were scarified in the name of security, with little promise of recovery. Stephen Graham's rich tour of what he describes as "the new military urbanism" paints a dismal picture of how these particular dynamics have reworked infrastructures across the globe.[35] Graham recounts how a novel focus on homeland security is leading to the adoption of military technologies and techniques into the conduits of everyday life—infrastructures, once communal and public spaces, are transformed into sites of fine-grained surveillance and control. Graham is not alone in this view; others have also documented in detail how the fear of terrorism props up new forms of surveillance and control that are built into the day-to-day operation of infrastructure.[36] This is the conventional narrative of post-9/11 politics—security fears run amok trample democratic norms and institutions and buttress illiberal constellations. Yet, as the following pages will make clear, the reality of post-9/11 infrastructure and post-9/11 politics is much more complicated and varied. The politics of risk have not only been put in service of the powerful but have worked to democratize and open infrastructure to new voices and new forms of public accountability. This is a counterintuitive finding. The threat of terrorism has been used to *pry open* infrastructure. A cross section of groups, including labor, environmental groups, city and state officials, and others used the vernacular of the war on terror to build out new coalitions and argue for new, enriched forms of public accountability. During the 1970s the language of the market was embraced as perhaps the only legitimate way of discussing or making sense of infrastructure; after 9/11, however, the language of security provided a new vocabulary. The risk of terrorism was not only invoked by the powerful to extend a tight grip over infrastructure. It was also used in nearly the exact opposite fashion: groups that were shoved to the side or fenced out of key decisions thanks to decades of political and economic restructuring now, suddenly, used the threat of terrorism as a way to successfully insert themselves into (or back into) the governance of infrastructure. In some cases these groups were able to enact meaningful change to how infrastructures operate. For example, the creation of new regulatory powers and standards covering the electric power grid and the transportation of toxic materials has enhanced public accountability in significant and durable ways. It has carved out spaces where interested publics and their representatives can now peer inside the workings of infrastructures and have a meaningful say over how they operate. These are not fleeting or minor changes. Through continual review, enforcement, and rulemaking efforts, regulatory bodies create a record of how infrastructures operate and provide ongoing opportunities for concerned publics to have a say.

The cases assembled in this book challenge familiar readings of post-9/11 politics. The securitization of infrastructure, as the following chapters make clear, was and remains a contradictory process. Reframing infrastructures as security problems leads to both conservative changes that reify and extend existing structures of power and important reversals that open infrastructures in a new and surprising fashion. Accounts that highlight the alarming ways in which counterterrorism and homeland security strategies have bolted military-style strategies onto civilian circuits of exchange are not wrong—but they are incomplete. As the case of the postal system, freight rail network, and electric power grid make clear, the risk of terrorism was, above all, flexible: different groups adopted it for different purposes with different lasting implications. Focusing on the ways in which postal workers, environmental activists, and other groups appropriated the language of the war on terror offers an important observation: the threat of terrorism was used as a tool by those at the margins to split open infrastructure governance and demand that their voices and their concerns be heard. Homeland security as a policy trope and a broader rhetorical framing did not only serve to reinforce the power of those who were already powerful but also served to check and call to account power in important, if overlooked, ways.[37]

Putting the contradictions of contemporary infrastructural changes under a powerful lens helps clarify and extend our knowledge about the political possibilities and limits of risk. Novel risks have a rich—if unpredictable—political power. As Langdon Winner ruefully observed nearly three decades ago, narratives of real and imagined physical harm offer one of the few ways in which technological systems can be meaningfully pulled out of the seemingly neutral world of technology and thrust into the world of politics and critique.[38] But the political possibilities of risk are undetermined. Risk can be used or deployed to serve quite different ends. This is true even of questions of national or geostrategic security, a domain often thought to be rigid and closed. The framing of topics under the rubric of "national security" is typically seen as a way of short-circuiting the normal processes of democratic governance. It is seen as a trump card that allows national security interests to drive out all other voices, ideas, and values.[39] But other dynamics are also possible. As legal and organizational scholar Mariano-Florentino Cuéllar cautions, the politics of security are not monolithic but contradictory and open.[40] The competition to define the outlines of what counts as a security problem is rampant and consequential. As Cuéllar notes, the concept of security is "to some degree malleable," making it difficult to chisel "tidy distinction between geostrategic national security and other types of safety and security."[41] Different topics and areas of concern can be—and often are—framed through the lens of security. In Cuéllar's reading, it is important to avoid "assuming an unusual degree of insularity and consensus in the security space" and instead focus on how particular individuals, coalitions, and interests work to translate security concerns into durable practices.[42] This is vital: focusing on the empirical question of how different groups and individuals work to maneuver the public organizations that actually translate broad, high-level concerns over security into tangible practices is essential. Securitization can spin out in different directions with different implications. Indeed, terrorism has been used by a heterodox collection of actors and coalitions to support a broad array of interests. It has been used to both bolt shut and jolt open infrastructure. These contradictions demonstrate the elasticity of securitization and the fragile possibilities of what sociologist Ulrich Beck refers to as *reflexive modernization*, a process through which novel risks create the scaffolding for new, engaged publics and new forms of political engagement that take aim at the overlooked political choices that sit at the heart of modernity.[43] Tracing the twists and turns of post-9/11 infrastructural upheavals shows that risks can lead to new forms of democratization while offering a bracing reminder that such transformations are by no means inevitable. What ultimately matters are how actors define and fashion particular notions of risk into working coalitions and laws, rules, technologies, and practices. Examining the remaking of infrastructure challenges the ways we often think about post-9/11 politics. It is not a tidy narrative but a story told in fragments: moments of revitalized democratic possibilities and checks on power sit side by side with efforts to dampen public participation and intensify existing hierarchies of power and control.

Theoretical Foundations: Making Sense of Infrastructure

The book borrows liberally from a variety of disciplines and bodies of knowledge, including sociology, political and economic history, science and technology studies, communication studies, and other fields in order to make sense of infrastructure. At its core, however, the investigation is rooted in the insights and possibilities of critical scholarship on infrastructure. Over the past several decades, scholars have created a body of work that takes as its starting point the critical investigation of infrastructure. These efforts, led by Thomas P. Hughes, Susan Leigh Star, Geoffrey Bowker, Paul Edwards, and others, have developed a number of key insights that inform the book.

As a starting point, it is useful to consider the following: What exactly is *infrastructure*? It is a deceptively tricky term to pin down. Geoffrey Bowker and his coauthors give us a useful and elastic initial definition, defining infrastructure "as a broad category referring to pervasive enabling resources in network form."[44] In other words, *infrastructures are systems that support other forms of activity*. This definition is expansive. It includes both physical systems as well as social forms such as the organizations, standards, and protocols that are involved in the provision of these systems. This definition is echoed in current U.S. law and policy. The 2013 Presidential Policy Directive on infrastructure protection offers a similar perspective, stating that "infrastructure provides the essential services that underpin American society."[45] This notion—that infrastructures are systems that sit beneath or "underpin" other forms of activity—is a useful point of departure. It captures the various examples explored in the book, and it also matches how scholars, policy-makers, and others often think about infrastructure.

Moving forward, a few important additional guiding concepts can help flesh out this bare concept. Three core observations drawn from the larger corpus of infrastructure studies help further define how the book approaches and makes sense of infrastructure.

Infrastructures Are Sociotechnical Systems

Infrastructures are bundles of hardware, software, laws, regulations, and ad hoc rules; they join together material systems and the larger world of institutions, organizations, and implicit and explicit assumptions.[46] Treating infrastructures as sociotechnical systems widens the analytic aperture and captures infrastructures as more than just assemblages of technical components. The power grid is often described as the world's largest and most complex machine.[47] It is made up of over 180,000 miles of high-voltage transmission lines; 21,437 utility-scale generators that convert coal, petroleum, natural gas, wind, and other sources of energy into electricity; more than 6,900 individual power plants; and myriad substations, transformers, circuit breakers, and switches (to say nothing of the fiber-optic cables, hard drives, monitors, remote terminal units, general and specialized software packages, and other computer and communications equipment essential to keeping the grid up and running).[48] The power grid is, of course, a technical system. *But it is not only* a technical system. It is also a $390.3 billion industry.[49] It is a world of complementary and hostile organizations—private utility companies providing electric power for a price; publicly owned electric cooperatives providing power at cost; state public utility commissions (PUCs) that regulate certain aspects of the electric power grid; federal regulators, which regulate certain *other* aspects of the electric power grid; nonprofit regional transmission organizations (RTOs) and independent system operators (ISOs) that manage and coordinate the grid's transmission network (the key connection that links power generation and local distribution networks); manufacturers that develop and sell all matter of components, from large power transformers that cost more than $7.5 million and weigh over 400 tons to the envelopes used to mail utility bills to customers; and advocacy organizations devoted to any number of issues, including protecting the environment, protecting the fossil fuel industry, protecting consumers, and protecting (after a fashion) the regulators (that would be the National Association of Regulatory Utility Commissioners).[50] The power grid is also a system made up of formal and informal standards and rules. These include state and federal laws, regulations formulated by regulatory bodies, voluntary guidelines developed by industry, and all manner of shorthand used by those working to keep the lights on. Electric power is also a cultural artifact. As David Nye's *Electrifying America: Social Meanings of a New Technology, 1880–1940*, cataloged 30 years ago, it is an artifact freighted with shifting values and meanings.[51] Nye's description of electric power is a fitting epithet for infrastructures as sociotechnical systems: "Someone owns it, some oppose it, many use it, and all interpret it."[52]

Treating infrastructures as *sociotechnical systems* recognizes that technologies are created, adopted, and defined within a broader social context. This is a simple but important point. This approach avoids overly technologically deterministic accounts that view technology as an autonomous actor that bends and shapes society to its will, and it avoids overly socialized accounts that view technology as infinitely malleable putty that is molded to the whims of various social forces and actors. A sociotechnical point of view, as used in this book, focuses on the ongoing interplay between technology and the larger world of organizations, institutions, and culture. It is in this intersection that infrastructures are created, sustained, and transformed. Technologies rarely appear fully formed. What in retrospect looks like a clear or linear trajectory from invention to later adoption and institutionalization is, in fact, filled with the messy stuff of history—competing technologies, unsettled uses, confused and unruly users, rival standards, and long-forgotten alternative ways of organizing and deploying a technology. Technologies offer a range of different possible uses or configurations, a set of different possible branching pathways, but it is left to organizations, institutions, and cultural understandings to clear, mark, and enforce these paths—winnowing down available options into a defined set of organizational forms, uses, and meanings. To make sense of how the post office, freight rail network, or electric power system were created, remade during the waves of deregulation that began in the 1970s, and then again remade after 9/11 requires mapping how infrastructures are at once social and technological formulations. The book takes as its starting point that infrastructures are more than wires, steel, and chips. They are a complex set of interacting technologies, organizations, institutions, and cultural assumptions. It is in this collision that infrastructures can be usefully analyzed and understood.

Infrastructures Are Relational

Infrastructures lash and bind infrastructure workers, owners, regulators, different types of users, and different sorts of uses into a particular set of relationships.[53] Power is central to infrastructure. No two groups are likely to relate to an infrastructure in the same way. Infrastructures create publics: groups defined in part by their connection to the larger systems. These different infrastructural publics see and relate to infrastructure in different ways.[54] The postal system offers a useful example. For letter carriers, the postal system is a job. It is a source of joy, frustration, sociability, economic support, and other workplace mundanities. For a rural community underserved by for-profit delivery services, it is a lifeline. It delivers medicine and other vital goods at comparably low costs. But for the staff at the Postal Regulatory Commission (previously known as the Postal Rate Commission), the postal system exists as a set of data to be scrutinized. Here, the postal system appears most readily as a collection of statistics on mail volume, processing costs, and other information deemed relevant for setting and adjusting rates. Direct-marketing agencies peddling circulars, political advertisements during the run-up to an election, and other postal ephemera see the postal system as an important way of reaching and selling access to targeted audiences. For some postal customers, the postal system is little more than a nuisance—a spigot distributing an unyielding supply of junk mail. Writing in 1970, Chief Justice Burger summarized this view well, noting that "whether measured by pieces or pounds, Everyman's mail today is made up overwhelmingly of material he did not seek from persons he does not know. And, all too often, it is matter he finds offensive."[55] To others, though, the postal infrastructure is a (still) cherished source of connection—it is the seemingly magical system that brings a child a birthday card from an out-of-town grandparent.

Different groups relate to infrastructure in different ways. Infrastructures are, as noted above, platforms for other forms of activity. But they are not neutral platforms. They organize a mix of users, uses, owners, workers, and regulators in a particular set of relationships. Digging even an inch under the surface of infrastructure reveals power and hierarchy. Certain users get favorable terms, while others face subtle and overt barriers to access and additional costs. Various types or work are rewarded, while other forms are viewed as disposable or unacknowledged. Particular types of uses are valued and promoted at the expense of others. Workers, owners, regulators, and customers rarely agree on the best or most equitable terms of infrastructure operation. Each makes different and at times competing claims regarding how the system should run and what its purpose or importance is. The book places power and control at the center of its analysis. In examining the twists and turns of these various systems, it sees infrastructures as sites of ongoing conflict. As Finn Brunton's history of unwanted electronic mail—spam—details, technologies are spaces of significant *drama*.[56] Brunton, following Bryan Pfaffenberger, identifies technologies as stages for social and political arguments precisely because they organize and distribute power.[57] Different interests spar and seek to renegotiate the organization and arrangement of these various infrastructural relationships.

This book is particularly interested in the interplay between organized interests (corporations, regulatory bodies, advocacy groups, and others), larger cultural narratives, and infrastructural control. The transformation of infrastructure into dangerous things after the terrorist attacks of 9/11 was in part a cultural upheaval (as was, to a degree, the reimagining of infrastructure during the last quarter of the 20th century as free market avatars). What is most fascinating, however, is how organized interests worked to leverage this newly salient cultural meaning of infrastructure to rework the laws, regulations, and technologies that make up these important sociotechnical systems.[58] Larger cultural narratives and logics are powerful, but they need allies—identifiable actors—to forward these ideas and shape them into concrete programs. The book focuses on how competing groups advance different claims to infrastructure and seek to alter the ways they stitch together heterodox groups and uses into a larger fabric. Conflict and power are central points of focus throughout the text.

Infrastructures Are Historical

Infrastructures are shaped by decisions that occurred decades, if not centuries, earlier at constitutive moments. In other words, infrastructures are path dependent. Once a particular way of organizing an infrastructure is in place, it becomes difficult to shift gears and enact meaningful, large-scale change. Richard John and Paul Starr identify these dynamics in U.S. communications history. They observed that once in place, particular models of governing the postal system, telegraph, and telephone were difficult—though not necessarily impossible—to change.[59] Thomas P. Hughes and Richard Hirsh identify similar path-dependent processes at work in the electrical industry.[60]

The overlapping legal, regulatory, and platform aspects of infrastructure work in favor of path dependency. Each of these features contribute to the "stickiness" of infrastructure. First, infrastructures are, in part, enshrined in law. Statutes touch on various aspects of infrastructure operation. Laws relating to infrastructure, like all laws, are difficult to change. As Paul Pierson argues, law itself is path dependent: majoritarian politics creates collective action challenges that ultimately favor keeping existing laws and legal regimes in place.[61] It is easier to live with the current law than to collect the votes needed to enact something—anything—new. Second, regulations also contribute to infrastructure inertia. Regulations are seemingly easier to alter than laws. Regulations formulated by regulatory bodies or rules enacted by administrative agencies do not always face the same degree of collective action challenges that confront the creation or modification of laws. Changing specific regulations does not necessarily require congressional authorization. Depending on the particular regulatory body, the agreement of a majority of regulatory commissioners is often all that is needed, a lower bar than what is required to enact legislation. But regulations also have inertia. Law and regulations help to organize infrastructure in certain ways. They favor some groups over others. Once particular regulations are in place, the constituencies that benefit from them fight to keep them in place. Interest groups cajole, pressure, and otherwise work to ensure that regulators maintain the status quo, helping to buttress the collective action challenges that favor the status quo. Third, the nature of infrastructures as platforms is a key contributor to path dependence. Generally, infrastructures underlie vast industries. These industries may, from time to time, push back and challenge existing laws and regulations, but there is a bias in favor of the status quo. This is due both to the fact that regulatory stability is preferred over unpredictable and sharp changes and, most importantly, because the legal and regulatory foundations of infrastructures are reproduced in the very structure of the industries that sit atop infrastructures. In other words, particular legal and regulatory outlines become chiseled within the larger industrial outlines. Take, for example, the freight rail industry during the late 1800s and early 1900s. After cycles of boom and bust, laws and regulations devised by the Interstate Commerce Commission (ICC) moved to stabilize a particular version of the rail industry—they protected large national and regional cartels (over diverse ownership); they favored shipments of raw materials over finished goods; and they favored protecting existing track and lines over consolidation and abandonment. Once these legal and regulatory protections were in place, organized interests, the railroads, key shippers, and others fought to keep them in place. The laws and regulations made these interests more powerful, which in turn intensified their advocacy for the status quo and made change more difficult. The particularities of law and regulation became increasingly rigid as they became ground into a set of ever more powerful complementary organizations. These overlapping legal, regulatory, and platform aspects of infrastructure contribute to path dependence. That is not to say, as we will see, that significant structural changes are impossible. It just means that such changes are difficult and rare.

The book focuses on three key constitutive moments: (1) the initial formation or consolidation of infrastructure, (2) the deregulation of infrastructure during the 1970s–1990s, and (3) the reordering of infrastructure after 9/11. Each of these three moments are important because they shaped these sociotechnical systems in important and transformative ways, creating pathways that would endure for significant periods or, in the case of the post-9/11 changes, appeared as though they would be difficult to change. Focusing on these moments underscores a key feature of infrastructures: they are historical artifacts. They are a palimpsest of long-ago decisions. Choices made for good, obscure, or poor reasons over time become engrained in the workings of infrastructures. Looking closely at these various key periods highlights both the durability of infrastructural orders and the ways in which they can, under certain conditions, become reversed or altered.

These three features of infrastructures—*infrastructures as sociotechnical systems*; *infrastructures as relational*; *infrastructures as historical*—guide the investigation that follows.

Theoretical Foundations: Making Sense of Risk

The concept of risk is also central to the book. How are particular objects made dangerous? How and why are certain hazards prioritized as political problems, while others are dismissed? The book takes risk to be a socially constructed material and discursive artifact. As developed here, this view of risk focuses on power—how power can create risk and how risk can, at times, serve to provide the political capital needed to confront entrenched power. This approach breaks with classic accounts of risk in economics and hews more closely to the sociological treatments of risk found in Charles Perrow's theoretical work on *normal accidents* and in Ulrich Beck's concept of *risk society*.[62] Perrow and Beck make a somewhat unusual pairing: Perrow's work is empirically detailed and focuses on the concrete ways in which organizations create new types of risk; Beck is prone to sweeping theorizing and is interested in how certain types of risk create new political possibilities. Taken together, however, they allow us to look at the consequences of deregulation and explore how risk circulates as a cultural and political resource.

In his foundational economic text, *Risk, Uncertainty, and Profit*, Frank Knight offers a straightforward definition of risk: risk is a measurable type of uncertainty.[63] It is a future possibility that can be calculated through the accumulation of historical data or other quantitative means. It is the calculation of the likelihood (and severity) of a given future event.[64] Against this notion of risk as something that can be calculated, Knight presents *uncertainty*: possibilities that resist quantification.[65] In lay conversation, Knight points out, these two phenomena—risk, which is measurable, and uncertainty, which is not—are often incorrectly blurred.[66] This notion of risk, as Andrew Lakoff notes in his overview of the concept, underlies techniques of technical risk assessment.[67] These techniques have been deployed by governments to determine and improve the welfare of populations against disease, accidents, and all manner of misfortune.[68] This approach to risk, as Lakoff reviews, has been criticized on a number of fronts. Most significantly, science and technology scholars have questioned the ways in which technical risk assessment masks hidden assumptions and values and marginalizes lay knowledge.[69] That is, it obscures or ignores power.

The work of Charles Perrow offers a useful way of examining risk from a different angle. Perrow is most interested in the intersection of organizations, power, and risk. Perrow coined the term *normal accidents* to describe failures rooted not in operator error or pure chance but rather in systemic properties.[70] In this view, systems that are tightly coupled and complex create the conditions for normal accidents. These accidents are "normal" not in the sense of frequently occurring but rather because they are the expected results of particular forms of systemic organization.[71] This is far afield from Knight and classic risk assessment. It says little about frequency or likelihood and concentrates instead on the possibilities of failure. It focuses on how systems become vulnerable or prone to failure, rather than the creation of tables recording historical incidents. Normal accident theory offers a vocabulary to qualitatively examine technical systems and organizations. In particular, it provides a way of thinking about and assessing the materiality of risk while still acknowledging that these risks are, at bottom, socially constructed; it offers a framework to examine how the various ways of arranging the technical and organizational outlines of systems have different possibilities of failure. In the pages that follow, this framework helps to make sense of and evaluate the material changes that occurred within the post office, rail system, and electric power grid. We can plot these systems as they move from loose to tightly coupled and from linear to complex. As they move across these planes, new forms of failure—including accidents, complications from natural disasters, and even terrorism—are now made possible or expanded. The adoption of centralized processing plants, just-in-time delivery models, complex software, and other changes can be scrutinized through this lens. But Perrow offers something larger than just a framework for assessing the material foundations of risk: he offers a reminder to connect the organization of these technical systems to larger currents of power. His work makes this point plain: material systems are socially constructed—they reflect and are defined by the organizations and larger political and economic institutions that surround them.[72] Technologies cannot be wrenched from their larger organizational and institutional context. To understand why or how a particular system becomes vulnerable in new ways requires working through the connections between organizations, institutions, and power. This book works in this spirit, using normal accident theory to evaluate or make sense of the ways in which deregulation reordered infrastructure.

Normal accident theory is helpful in evaluating how deregulation transformed the post office, freight rail system, and electric power grid into vulnerable configurations. But it says little about how these systems and their attendant risks became public problems or how these risks were ultimately translated into particular security practices. Here, the work of Ulrich Beck is indispensable. While Perrow focuses on the social construction of material risks, Beck offers conceptual tools to explore how risk circulates as a cultural artifact and political resource. Beck argues that contemporary life is in the process of becoming a risk society.[73] Modernity is creating new forms of risk that cannot be calculated and managed through the usual tools of government and science.[74] These new forms of harm are incalculable, potentially catastrophic, and, importantly, generated by the very processes of modernization. Beck argues that these sorts of risk are politically explosive.[75] They can serve as the foundation for new political coalitions and new ways of organizing. They can lead to the democratization of areas of social life—such as the economy, fields of science and technology, and politics—that are shut. But these are only possibilities. Beck is quick to point out that risk on its own cannot compel anything—it requires groups to mobilize and work to translate the political possibilities of risk into durable and specific programs.

Beck's account is useful in highlighting how infrastructure risk circulates as a volatile and promiscuous political resource. His work can help to better understand how the post office, freight rail network, and electric power grid became salient problems. Now we see the overlapping cultural, organizational, and institutional processes that worked to highlight these particular risks (over myriad others) and transform these systems into objects of concern and, ultimately, action. Perrow can help us map how these systems became prone to new forms of failure, but Beck assists in sketching how these possibilities became salient and politically transformative. Taken together, Perrow and Beck offer useful points of departure for thinking about the contemporary reordering of infrastructure as dangerous things.

The Structure of the Book

The main body of the text is divided into two broad thematic sections. Part I, "The Political Origins of Infrastructure Vulnerability," explores the social and material impacts of the regulation and eventual deregulation of the postal system, freight rail network, and electric power system. Part II, “Ubiquitous Targets: Infrastructure Security after September 11,” examines the post-9/11 remaking of these infrastructures. It considers how new anxieties over terrorism and infrastructure subversion worked to transform each of these sociotechnical systems. Here, the book documents the *bureaucratization of risk*: how fears over terrorism were translated and encoded into new laws, regulations, technologies, and practices. The conclusion and coda examine the importance, limitations, and contradictions uncovered within these three specific case studies.

Chapter 1, “Stumbling toward Resilience: The Overlooked Virtues of Regulation,” examines the historical foundations and practice of regulation within the postal system, electric power grid, and freight rail network. Regulation appeared in a slightly different guise across each system. In each case, law and policy shaped the social and material outlines of these systems in specific ways. Regulation offered a degree of public accountability over infrastructure: it organized the warring set of competing interests—different infrastructure publics—that surround these networks and carved out a space for public participation in infrastructure governance. Regulation also directly and indirectly shaped core decisions concerning the material organization of these systems—the broader structure of regulation found expression in these systems’ smallest details. Chapter 1 uncovers the hidden and not-so-hidden benefits tucked within the old regulatory models. In addition to stabilizing these systems and providing the public with venues to air their concerns, regulation, in its various forms, worked to promote resilient systems. Regulation supported systems that were fault-tolerant: failures (from accidents, natural disasters, or intentional disruption) were local in scope and limited in size. Chapter 1 introduces normal accident theory, a key touchstone for the rest of the text, in more depth.

Chapter 2, “The Political Origins of Infrastructure Vulnerability: The Hidden Vices of Deregulation,” turns to examine how deregulation remade the postal system, freight rail network, and electric power grid. Political restructuring led to a host of social and material changes. Deregulation was incomplete: although state supervision was not entirely swept away, on balance, reform drastically renegotiated the balance of power between the state and various infrastructure publics. The chapter traces how restructuring gave key market players enormous new power to define how these infrastructures operated while leaving other groups on the side. Deregulation also led to the gutting of support for resilience. It promised to sweep away the inefficiencies of the old regulatory model and sought to create new lean infrastructures trimmed of the “fat” that had accumulated under state stewardship. But these changes came at a price. Political restructuring pushed these systems into increasingly combustible formations. Chapter 2 reveals the hidden and overlooked costs of deregulation. The drive to improve efficiency created systems that were ripe for large-scale failure and increasingly sealed off from substantive public control. It was precisely these new possibilities of failure that would reappear after 9/11 as pressing and difficult public problems, and it was this power dynamic that would be tested and, in some cases, upended through new forms of infrastructure security.

Chapter 3, "Imagination Unbound: Risk, Politics, and Post-9/11 Anxiety," considers the interlaced post-9/11 cultural, institutional, and organizational changes that worked to transform infrastructure vulnerabilities into public problems. The material changes ushered in through deregulation created new possibilities of failure, but these material reorderings were only legible as security problems thanks to the changes enacted after 9/11. Now, infrastructures were viewed through the lens of the war on terror. The development of homeland security policy helped legitimize the notion that infrastructure can and should be thought of as dangerous objects in need of protection—a key cultural shift or reshuffling. Organizational and institutional changes supported this conception of infrastructure and set the stage for the fractious battles over how, exactly, new forms of security would be put into place. This chapter looks closely at the work of Ulrich Beck and spotlights the important social changes that underlie the transformation of infrastructure into dangerous things.

Chapter 4, "Infected Mail: Labor, Commerce, and the 2001 Anthrax Attacks," begins a series of three chapters that focus on how new forms of security were invented and deployed within each infrastructure sector. This chapter focuses on postal security. It critically investigates the new security practices that the United States Postal Service (USPS) put into place after the 2001 anthrax attacks. Eventually, USPS adopted two new systems: the Biohazard Detection System (BDS) and Intelligent Mail. Postal management, labor, large commercial mailers, defense contractors, and local communities fought bitterly over the terms of postal security. Labor used the threat of terrorism to open up postal governance and secure access to high-level technical advisory boards. These gains, however, were short-lived and modest. Ultimately, the interests of large commercial mailers were encoded within the architecture and operation of both the BDS and Intelligent Mail. Chapter 4 examines the minutiae of these surveillance systems and uncovers the retrenchment of powerful interests at the expense of postal labor and the larger public.

Chapter 5, "Green Security: The Environmental Movement, the Transportation of Hazardous Materials, and the War on Terror," examines the creation of new security regulations governing the rail shipments of hazardous materials. Chapter 5 charts how activists—for example, Greenpeace, Friends of the Earth, the Sierra Club—local public officials, and select members of Congress adopted the vernacular of the war on terror in order to secure tougher controls over shipments of hazardous materials. The threat of terrorism provided a new rallying point for environmental activists and a new means of building an effective policy coalition. It allowed previously marginalized actors to assert their voices, to overcome stiff opposition from rail and chemical lobbies, and, ultimately, to substantively change transportation law and policy. While chapter 4 offers a window into how the political possibilities of risk can be put into the service of the powerful, this chapter highlights how marginalized groups can leverage the risk of terrorism to check the power of market players and create new forms of accountability over infrastructure.

Chapter 6, "Regulating Cybersecurity: The Unexpected Remaking of Electric Power," sketches the development and implementation of new cybersecurity regulations for the electric power grid. These regulations grew from what initially appeared to be industry-friendly legislation and thin administrative powers into a robust system of public accountability. Here, as in chapter 5, risk provides a key political resource that was put into service to address the material vulnerabilities and social transformations of deregulation in a meaningful way. The expansion of regulatory authority effectively democratized infrastructure governance. Under the newly adopted regulatory regime, the public, regulators, and concerned parties can now participate in the draft, review, and implementation of mandatory standards. Rather than having decisions over the grid decided by industry through closed-door negotiations, the process is transparent and accessible.

The book draws to a close with a short conclusion and coda. The conclusion, "The Politics of Critical Infrastructure Protection," steps back to review the three cases. After 9/11 the political project of deregulation was put on trial. The triumphant boosterism of free markets, corporate power, and a deferential state began to sound tin. Policy-makers wrestled with the consequences of deregulation and tried to patch new forms of security onto these vast and complicated sociotechnical systems. The conclusion takes stock of these efforts and finds the complicated legacy of 9/11 recorded in the intricate workings of infrastructure.

The coda, "Infrastructure as Target," expands the book's frame to look beyond infrastructure protection and security efforts and toward the development of offensive capabilities targeting infrastructure. While U.S. policy-makers and other interested parties worked to design new forms of infrastructure security, the government also worked to create new, secretive, state-sponsored tools of espionage and sabotage that threatened to undermine these gains. New intelligence-gathering techniques and hacking tools threaten infrastructure security both at home and abroad. The coda examines the U.S. defense and intelligence communities' efforts to weaken encryption standards and create stockpiles of previously unknown and undisclosed software vulnerabilities—what are known as *zero-days*. The text documents how efforts to target the infrastructure of our adversaries (and even, sometimes, our allies) can undermine the security of domestic networks. While the U.S. is spending tens of billions of dollars annually on critical infrastructure protection, deep in the "black budget" are efforts designed to preserve flaws, prevent the adoption of robust protections, and, generally, promote insecure systems. The coda considers the tension between homeland security and the creation of tools that target infrastructure for offensive purposes. The book draws to a close with a mordant question: Is the best defense, perhaps, a weak offense?