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

Conclusion: The Politics of Critical Infrastructure Protection

The recasting of infrastructures as dangerous things was—and *is*—potent. It created a moment of political reflexivity, an opportunity to revisit and reorder the material and organizational foundations of infrastructure. *Infrastructures always order*: they inevitably prioritize certain users, certain uses, and particular visions of these systems over others. Security offered a way to alter how different infrastructure publics—particular customers, operators, regulators, advocacy groups, and others—relate to one another. It promised a reconsideration of which publics, uses, and imaginings of infrastructure would be prioritized and which would be marginalized.

The postal system, the freight rail network, and the electric power system have each been transformed. Additional layers of security technologies, regulations, standards, and practices now govern these systems. Once novel and contentious, these practices have become a regular and largely taken-for-granted part of these infrastructures. These changes are dramatic and uneven: dramatic in the sense that they sprang from high-stakes and deeply contested battles between various infrastructure publics, and uneven in that the outcomes of these dramas, these fights, are ultimately mixed. The reframing of these systems as dangerous things allowed for the larger set of political choices built into these systems to become visible and open to debate. Decades of political and economic reform—deregulation—pushed these systems to the brink. It stripped away key mechanisms of public oversight *and* created new forms of systemic vulnerability at the core of these networks. The recasting of infrastructures as dangerous things created real possibilities for change. It offered the chance to reckon with the consequences of deregulation. It offered the opportunity to revisit and remake the status quo. It offered the chance to shift power within these systems. It offered the opportunity to address the material vulnerabilities that sat at the center of these infrastructures. The

complex transformation of infrastructures into dangerous things after 9/11 offered (and might still offer) this and more. It offered possibilities. *Possibilities*. Not certainties.

The refashioning of the postal system, freight rail network, and electric power grid followed two very different paths. In freight rail and electric power, something surprising happened. New security practices reordered power within these networks. Groups that had been pushed to the margins found in the post-9/11 vernacular a new voice and a new way of organizing. New regulatory powers, rules, and practices now provide a degree of public accountability that had withered or gone missing. These changes are at odds with how we most often think about post-9/11 security politics. Security concerns in these cases did not feed increased secrecy; they did not lead to the further consolidation of power in the hands of the few; they did not lead to the erosion of democratic norms; and they did not lead to ineffective security theater. They led to new forms of public accountability. The adopted regulations check the power of incumbents and key customers to control infrastructure. They are a counterweight. The now-in-place regulatory powers offer the opportunity for public officials to scrutinize, review, and push back against decisions made by influential corners of industry and, importantly, they provide an opportunity for *other* infrastructure publics to do the same. The regulatory process is open. It invites comment and review from a diverse array of players. Powerful electric power companies or railroads cannot simply set their own rules. They are pushed into dialogue with other publics whether they like it or not. The adopted regulations enable public accountability because they allow multiple competing publics an opportunity to examine how core infrastructure operators work; they acknowledge the plural publics that are bound together through infrastructure; they offer a venue for different publics to advocate for their interests; and they embrace a logic—a way of interpreting and making decisions about how infrastructures *should* operate—that is open to competing values and interests and not simply subservient to the demands of the market.

These changes are not just smart politics that are laudable for their inclusive bent. They also address the material vulnerabilities that decades of political and economic reform helped to create. In freight rail, the adopted changes reduce the risks associated with the transportation of dangerous cargoes. Decades of political and economic reform encouraged bulk shipments of hazardous materials along the most cost-efficient routes possible, bringing them through cities and tightly packed areas. This generated real risks. This type of *spatial dependency*, fusing together

the city and the transportation of bulk shipments of hazardous materials, creates the potential for catastrophic releases.[1] The adopted security regulations work to break these connections by pushing bulk shipments away from populated areas. This is a significant reversal. Security regulations force rail companies to consider something other than the bottom line in making routing decisions. The story in electric power is very much the same. The Critical Infrastructure Protection (CIP) standards address serious risks in a useful way. The evolving CIP standards work to limit the vulnerabilities related to the integration of generative networked computers within electric power. Deregulation hastened the adoption of this particular model of computing and networking, while also binding together power systems into larger configurations. The CIP standards push back. They work to isolate or segment operational technology from other larger multipurpose networks and require companies to inventory their assets and adopt limits and controls on how they might be used. These standards cannot turn back the clock to the world of single-purpose machines and dedicated networks. But they do work to reduce risk. The splintering of power within these infrastructures—bringing many different publics back in—improves security.

The rail and electric power cases paint a rosy picture of how infrastructure fears, backed by a set of supporting institutional changes and stout organizational advocacy, can translate into new forms of public accountability that carry both political and security benefits. The case of the postal system tells a different story. Here, power is not reordered: existing hierarchies are further entrenched. The aftermath of the anthrax attacks for a moment appeared to offer postal workers the chance to seize new powers to dictate postal policy. Suddenly on the "front lines of the war on terror," labor challenged the power of commercial mailers to define postal policy and sought security solutions that would protect them from harm. But the hopes of workers were dashed. Any sort of larger transformation was ultimately fleeting: new forms of security did not upend the status quo. On the contrary, security practices cement the prominent position of a cadre of commercial mailers at the expense of postal workers. The Biohazard Detection System (BDS) and Intelligent Mail program serve the interests of large commercial mailers. The benefits of these systems are partial. The health and safety of workers are traded away in favor of lower costs for bulk mailers, new tools engineered to help aid the adoption of temporary noncareer (nonunion) workers, and new, informational postal products pitched to industrial customers. Postal employees might have been able to claim they were on the front

lines of the war on terror, but new forms of infrastructure security are more worried about the bottom line of commercial mailers than the well-being of workers. The recasting of infrastructures as dangerous things is ripe with the potential for change. But, as the collected cases make plain, the shape and form these changes can take are very much open.

What are we to make of these contradictory changes? These vignettes complicate our understanding of post-9/11 security politics and the political power of risk. These cases do not necessarily fit the usual or familiar ways in which we think about or understand the politics of infrastructure security. These cases are not, in the main, stories about security theater. Nor are they only stories about how already powerful groups—government or industry—use catastrophes to enhance their already substantial powers. These cases offer a different picture. The risk of terrorism became a powerful rallying cry that served multiple ends. Marginalized groups used it to reckon with the consequences of decades of political and economic reforms. Fears about these dangerous things were translated into new forms of public accountability. These changes address real systemic vulnerabilities and reorder power. They open infrastructure to different publics. New forms of security, in the cases of freight rail and electric power, are something of a restoration. Decades of political and economic reforms removed the key mechanisms that provided public oversight of infrastructure. Now, oversight is reinvigorated in the guise of security. Yet sitting side-by-side with stories about the transformative power of risk is the case of the postal system. Sometimes risks *do* serve the powerful. Sometimes fears are translated into practices and tools that further entrench the powerful. Sometimes the familiar story also happens to be true. Taken together, these cases are fragments that complicate our understanding about the contradictory post-9/11 world that we still are living in, and they remind us that risks are unruly fissures that can run in multiple directions.

* * * *

Case studies are always partial glimpses into a larger world. They tell us something specific and, in doing so, point toward something larger. Shifting through these cases reveals larger themes and observations. These insights can help plot a path forward. The recasting of infrastructures as dangerous things remains very much alive. The threaded cultural, institutional, and organizational changes that came to the fore in the years after the terrorist attacks of September 11 and transformed infrastructures into dangerous things are still in place. The long shadow of

9/11 continues—nearly two decades later—to color how we think about, interact with, and make and remake infrastructure. The case studies offer insights that can be used to navigate and make sense of the politics of infrastructure security. Three key insights stand out.

Recovering the Sunk Politics of Infrastructure: The Importance of Historical Thinking

Infrastructures are monuments to the past. Contingent choices made decades ago become ossified within the inner workings of these systems. Decisions that are wise, foolish, or simply the product of happenstance can and often do reverberate within these systems for decades in subtle and explicit ways. It is easy to lose sight of the histories encoded within these systems. Forgetting is perilous. It makes it difficult to clearly understand the stakes that cling to contemporary infrastructure security interventions.

In each of the cases collected in these pages, choices made during the last third of the 20th century set the stage for the conflicts over infrastructure security that would arise at the start of the 21st century. Deregulation was a thorough transformation of the postal system, freight rail network, and electric power grid. The political and economic project of deregulation became distilled within each of these systems. The adoption of new centralized automated facilities in the postal system, the spike in hazardous materials carried by rail, and the integration of networked generative computers within electric power were each, in different ways, products of deregulation. These changes were not inevitable: they were the intended and unintended consequences of political choices. Political and economic reform was not simply contemporaneous with the adoption of automated postal machines or multipurpose computers within electric power: reforms drove the adoption and integration of certain technical components and elements within the larger network assemblage. The shifting mix of commodities handled by the railroads during the 1980s and beyond was not the product of immutable laws of economics: it was the product of legislative changes and related regulatory decisions about how to assign costs and markups. Political choices were reproduced within these networks in subtle (and not so subtle) ways. Later—but only later—these changes would become legible as the key drivers of systemic vulnerability. That is, they would become problems that needed to be fixed.

Individual infrastructure components embalm the past and carry it into the present. Identifying the role that larger historical forces play in shaping the material outlines of infrastructure is vital. It is more than just

understanding how or why a particular facet of a system came to be—it is a necessary element for sorting out the stakes of contemporary security conflicts. In the cases examined, drawing a thick line connecting deregulation and post-9/11 security efforts points out a core structural tension: the seeming incompatibility between the drive for increasingly efficient infrastructures under private control and the desire for secure systems. Identifying and understanding this tension is important. It crystallizes the larger ideological stakes and conflicts sitting beneath the surface. The documented security efforts cataloged here constantly run up against the thrust of the larger political and economic project of deregulation. Post-9/11 debates about infrastructure security were implicit and explicit referendums on deregulation. The overlooked costs of political and economic reforms came due. Recapturing the history sunk within these systems offers a reminder that infrastructure security is always about more than tinkering with the settings on a workstation at an electric power company, it is about more than figuring out what particular route a train hauling chlorine should take, and it is about more than determining which piece of automated sorting equipment should have an "anthrax smoke alarm" (as the BDS is sometimes known). It is about grappling with the collision between the politics of the past that have become encoded and drilled into the workings of infrastructure and the fast-moving onrush of the politics of the moment that seek to remake and revisit these systems.

Historicizing infrastructure uncovers the tension between the politics of the past and present. It draws out the larger ideological conflicts and political choices that sit behind security debates. The cases here looked at the tension between post-9/11 security anxieties and deregulation and revealed a rich irony: decades of promarket infrastructure reforms led to the need for increasingly intense state interventions to stabilize these systems. Future cases examining infrastructure security in various contexts will find surprising collisions between past and present. Historicizing infrastructure security underlines and makes visible the larger structural tensions that are at play. It offers a window into why efforts to remake infrastructures and bolt on new forms of security can be difficult and face stiff opposition. It provides a glimpse into how distinct political moments collide. In other words, it starts to clarify what exactly is at stake when infrastructures are made secure.

Infrastructure Orders: Infrastructure Publics and Their Problems

In focusing on infrastructure security interventions and efforts, the question "Do they work?" *must* give way to the larger question "For whom do they work?" Torin Monahan first proposed a similar reframing as a way of understanding and critiquing surveillance.[2] But this insight is just as relevant when applied to infrastructure security. Thinking through the practical impacts of security efforts—whether they succeed or fail in making systems more or less secure—*cannot* be disentangled from a larger reckoning with how security practices produce particular types of social relations. What counts as "secure" is always negotiated and provisional. It only emerges through the clash of battling infrastructure publics and competing visions about for what and for whom these systems are made.

In the wake of the 2001 anthrax attacks, a sharp contest between commercial mailers, labor, and management broke out. Each of these groups had its own priorities and saw security differently: commercial mailers wanted to reassure the public that the mail was safe while limiting any additional costs or delays to the mail; labor wanted a safe workplace and a greater say in postal policy, particularly as it related to how new technologies would be integrated into the mail system; and management wanted to keep the postal system viable in the face of its myriad economic woes and quell the bubbling panic from the attacks. These and other players wanted to create a secure system, but what that meant for each group did not always align. Each group related to the postal system differently. For letter carriers and clerks, the postal system was where they worked. It was a job. For commercial mailers it was a cheap, low-cost network that links advertisers with consumers. The postal system means different things to different publics. It is unsurprising, then, that what constituted a "secure" system also diverged for these groups.

Infrastructures create and bind together different publics. They fuse heterogeneous publics into a tentative hierarchy. Certain publics—as well as uses and infrastructural imaginings—are prioritized, while others are shoved aside. New security efforts invariably offer an opportunity to maintain or reshuffle these orders. They offer a chance to reconsider what publics matter, which visions count, and what uses are given priority over others. Security efforts order these publics, these visions, and these uses. They present different ways of arranging or prioritizing. Purely utilitarian frames—asking new security interventions such as "Do they work?"—elide too much: they ignore the different competing publics, meanings, and uses that are always contained and constrained within infrastructure.

Explorations of infrastructure security must be attuned to how security orders. The question "For whom do they work?" can usefully start this process. It places the multiplicity of infrastructure publics at the center of analysis and can reveal how producing a secure system is always about creating and affirming hierarchies.

The Promiscuous Politics of Security: Reflexive Modernization and the Power of Organized Interests

The case studies offer a reminder that risks are powerful *and* promiscuous resources. After the terrorist attacks of September 11, a number of key changes worked to transform infrastructures into dangerous things. President George W. Bush's framing of civilian infrastructure writ large as sites of danger and geostrategic security concern led an important cultural shift. This framing had circulated for decades during the Cold War and immediate post–Cold War era within think tanks and inside-the-Beltway policy circles. But the president's adoption of this frame gave it a new currency and legitimacy. Now it became acceptable and common to speak about infrastructure as targets-in-waiting. At the same time, the institutionalization of *critical infrastructure* security as a key priority through the creation of the Department of Homeland Security, the opening of spigots of federal and state funding devoted to this issue, and other changes ensured that this cultural reframing would become durable and powerful. This recasting, however, was not yet complete without the work of organized interests. Postal workers, environmental groups, electric utilities, and many others picked up on this framing and advocated for specific policies and practices. These changes—cultural, institutional, and organizational—transformed infrastructures into dangerous things. Deregulation may have created or enlarged systemic vulnerabilities, but these changes made these instabilities culturally and politically legible.

The collected cases paint an unfamiliar and contradictory picture of post-9/11 politics. The case of freight rail and electric power demonstrate how risks can serve as powerful catalysts for surprising political transformations and reversals. Typically, the politics of national security are taken to be antithetical to accountability and democratization. Security is often seen to be a trump card that can be used to extend the influence of the powerful; it is used to suspend normal democratic processes and, in their place, support exceptional powers. The cases in this book offer a more complicated portrait. In the cases of rail and electric power, the risk of terrorism was used to wrench open previously closed domains. Fears

over terrorism offered marginalized infrastructure publics a way to reassert their interests. Terrorism provided a scaffolding to build new forms of accountability that accommodated multiple different publics. In the postal case, as noted above, this did not happen. Here, a more familiar story unfolded: powerful players enhanced and extended their power.

These cases offer a reminder: risks are powerful, but promiscuous. They are always open to multiple competing interpretations. They can aid the powerful and the marginalized alike. Risks can create moments of instability, but how these moments are fashioned into lasting changes—the bureaucratization of risk—is always an open question. Investigations into infrastructure security must account for this promiscuity. Detailed empirical investigations into how organized interests work within a particular cultural and institutional milieu to harness the power and possibilities of risk are crucial. The preceding chapters provide an example of this type of study, mapping how moments of instability are first created and then fashioned into transformative or reactionary changes.

The Politics of Infrastructure Security

Infrastructures remain dangerous things. The particular set of cultural, institutional, and organizational changes set in motion after September 11, 2001, remains firmly in place. It is a powerful matrix. Security remains one of the primary ways in which we think about and shape infrastructure. The full implications of this recasting continue to unfold.

In the summer of 2018, President Trump held a rally in West Virginia. During his remarks, he offered a broad attack against renewable energy, stating: "In times of war, in times of conflict, you can blow up those windmills. They fall down real quick. … You can do a lot of things to solar panels, but you know what you can't hurt? Coal. You can do whatever you want to coal."[3] The symbolic use of national security—the language of war and conflict—to support a political priority is not new. President Trump's use of this trope to support coal—during a political rally deep in coal country—is not remarkable. Presidents freighted their causes with urgency by linking them to wars both real and metaphorical long before President Trump took office. But the weight and power of Trump's rhetorical invocation is different today than it would have been just two decades ago. The changes that followed September 11, 2001, make these sorts of calls powerful, regardless if they are justified or not. Here, Trump seemed to employ, in an offhand and difficult to parse manner, the language of national security to undermine support and investment in green

energy. This remark carries weight not just because the president uttered it but because there are now corresponding bureaucratic apparatuses (and billions of dollars) in place that support decisions about infrastructure based on notions of security that are elastic and fungible.

The relative "openness" of security makes it a powerful tool. It can be repurposed by different groups for varied ends. The idea that infrastructures are dangerous things sitting at the center of larger geostrategic conflicts remains salient. Infrastructure protection is now embedded within a web of institutions that are devoted to and prop up this idea. What remains to be seen is how organized interests will work within this terrain to advocate for new infrastructure orders. As the preceding pages make clear, security can be used to open infrastructures to multiple publics and different visions. It can be used to make infrastructures accountable to the various publics they create and bind. Or, invocations of security can be used as a tool to further marginalize: to seal off infrastructures to all but the most powerful voices; to elevate and embrace narrow sets of interests and imaginings of what these systems are for and whom they should serve. In other words, the recasting of infrastructures as dangerous things can be used to tear down walls or prop them up. The path that new and not yet waged battles over infrastructure security might take in the future remains undecided. Documenting how the powerful new cultural, institutional, and organizational context that surrounds infrastructure is translated into practice remains an ongoing task. The assembled case studies not only reveal the important changes and conflicts that mark these particular infrastructures but also offer a guide to an uncertain future and the infrastructural changes yet to come.