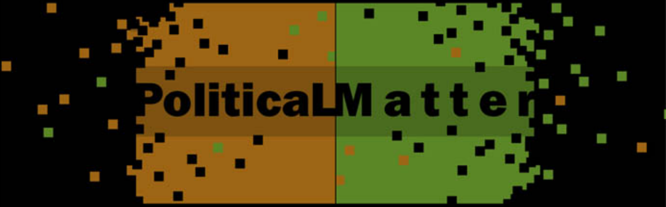
Political Matter



Technoscience, Democracy, and Public Life

Bruce Braun and Sarah J. Whatmore, Editors

POLITICAL MATTER

This page intentionally left blank

Political Matter

Technoscience, Democracy, and Public Life

Bruce Braun and
Sarah J. Whatmore, Editors

MINNESOTA
University of Minnesota Press
MINNEAPOLIS · LONDON

A version of chapter 2 was previously published as Jane Bennett, "The Force of Things," *Political Theory* 32, no. 3 (2004): 347–72. Copyright 2004 Sage Publications.

Chapter 3 was published as William Connolly, "Materiality, Experience, and Surveillance," in *New Materialisms,* ed. Diana Coole and Samantha Frost (Durham, N.C.: Duke University Press, 2010). Copyright William E. Connolly. All rights reserved. Reprinted by permission of the publisher.

Chapter 6 was published as Nigel Thrift, "Halos," in *Mobile Nation: Creating Methodologies for Mobile Platforms*, ed. Martha Ladly and Philip Beesley (Waterloo, Ont.: Riverside Architectural Press, 2008).

Published by the University of Minnesota Press
111 Third Avenue South, Suite 290
Minneapolis, MN 55401-2520
http://www.upress.umn.edu

Library of Congress Cataloging-in-Publication Data

Political matter : technoscience, democracy, and public life / Bruce Braun and Sarah J. Whatmore, editors.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-8166-7088-8 (hc : alk. paper) — ISBN 978-0-8166-7089-5 (pb : alk. paper)
1. Political science. 2. Technology—Political aspects. 3. Materialism—Political aspects. I. Braun, Bruce, 1964– II. Whatmore, Sarah J..
JA80.P63 2010
320—dc22
2010019695

Printed in the United States of America on acid-free paper

17 16 15 14 13 12 11 10 10 9 8 7 6 5 4 3 2 1

Contents

Part I. Rematerializing Political Theory: Things Forcing Thought

Part II. Technological Politics: Affective Objects and Events

Part III. Political Technologies: Public (Dis)Orderings

9 Infrastructure and Event: The Political Technology of Preparedness

ANDREW LAKOFF AND
STEPHEN J. COLLIER

As a number of analysts have argued, contemporary citizenship is simultaneously political and technical (see, e.g., Barry 1999; also contributions to Ong and Collier 2005). Thus, for example, access to material systems of circulation—such as water, electricity, communication, and transportation—is critical to participation in collective life. Indeed, demands for such access are often sources of political mobilization. This collective dependence on what we might call "vital systems" also fosters new forms of vulnerability. Threats to the operations of these life-supporting systems may come from a number of sources: natural disasters, terrorist attacks, technical malfunction, or novel pathogens. The prospect of such catastrophic threats now structures political intervention in a number of domains. Exemplary instances in which the failure to protect the functioning of such systems has caused major political fallout include the outbreak of mad cow disease and the European system of food supply, the attacks of September 11 and the system of air transportation, and Hurricane Katrina and systems of flood management. In this chapter, we describe the development of technical methods to identify and manage these threats to vital systems. The prevalence of these methods—and the common assumption of their necessity—suggests one answer to the question, how are political demands materialized today in programs of technical response? Through such methods, a range of significant "things" is internalized within political reason.

The chapter describes how critical infrastructure—and specifically the vulnerability of critical infrastructure—has become an object of knowledge for security experts in the United States. The production of such knowledge, we will suggest, is one part of a *political technology of preparedness* that addresses itself to a variety of possible threats. This political technology generates knowledge about infrastructural vulnerabilities through the imaginative enactment of a certain type of event. By the term *political technology,* we indicate a systematic relation of knowledge and intervention applied to a problem of collective life (Foucault 2001).[1] In this case, the political technology of preparedness responds to the governmental problem of planning for unpredictable but potentially catastrophic events. It works to integrate an array of material elements—ranging from switching stations to chemical plants to oil pipelines and network servers—into political organization.

Such political attention to the material underpinnings of collective life is not in itself new or surprising. Since the eighteenth century, experts have seen "the government of things" as one of the central tasks of state rationality (Foucault 2007). Thus current approaches in science and technology studies (STS) that draw attention to the salience of material artifacts to politics follow a long tradition of technocratic thought. From the vantage of critical analysis, what is important to specify is *how,* at a given moment, such technical artifacts as electricity networks are taken up as problems of collective existence: according to what rationality, and with what aim, do material things become political?

The chapter begins with a brief description of current critical infrastructure protection efforts in the United States. These efforts focus on mitigating perceived vulnerabilities to potentially disastrous events. It then turns to a key moment in which this relationship between infrastructure and event was developed—cold war civil defense. Here the chapter describes how the practice of "vulnerability mapping" worked as a way of generating knowledge about urban life in the shadow of nuclear attack. The chapter then follows the trajectory of imaginative enactment as a planning technique during the cold war and shows how this method of generating knowledge about vulnerability gradually extended to other types of threat. In closing, we suggest ways in which this story about recent developments in security expertise might be linked to broader discussions of the contemporary politics of technology.

Infrastructure and the Problem of Vulnerability

In a 2003 essay on "Infrastructure and Modernity," Paul Edwards posed the question of how to link detailed studies of the underpinnings of large-scale sociotechnical systems—which focus on issues such as the negotiation of standards and the problem of interoperability between systems—to questions raised in social theoretical discussions that emphasize the centrality of technological systems to modern life (Edwards 2003). He suggested that the differences between these two scales of analysis—one emphasizing the micropractices of technical experts in specific domains and the other making broad, general claims about modernity and technology—should, in principle, be reconcilable. This challenge is similar to the one posed by the editors of this volume, who have asked contributors to "draw questions of science and technology more fully into political theory, and to bring political theory to bear more consistently on our understanding of scientific practices and technological objects." In what follows we try to address these challenges by focusing on a specific technical domain, but one that responds to a broad political problem.

We focus on how experts in the management of risk have addressed the vulnerability of complex sociotechnical systems as a problem of collective security. This problem of system vulnerability is implicit in many current STS discussions of infrastructure. For example, Geof Bowker and Leigh Star (1999) emphasize that infrastructure is a fragile accomplishment and point to moments of breakdown as sites in which the work of infrastructure suddenly becomes visible. From a different vantage, the problem of system vulnerability is also central to social theories of risk, as in the work of Ulrich Beck (1999) on risk society. Beck argues that the very sociotechnical systems that were initially built to sustain human well-being as part of modern social welfare programs now generate new threats. Our dependence on these vital systems—energy, transportation, communication—is, for Beck, a source of vulnerability. His examples of threats that come from infrastructural dependence include ecological catastrophes such as Bhopal and Chernobyl, global financial crises, and mass casualty terrorist attacks. Such hazards, he argues, can cause global, irreparable damage, and their effects are of potentially unlimited temporal duration.

Our point in turning to Beck's argument here is neither to endorse nor to criticize its accuracy as a diagnosis of contemporary politics;[2] rather, it is to note a striking parallel between his diagnosis and that of a subset of contemporary security planners in the United States. For Beck, there is a broad class of contemporary threats—catastrophic risks—that outstrip statistical methods of management and control because their occurrence is unpredictable and their impact is unbounded. Moreover, he argues, it is our very reliance on modern technological systems that makes us especially vulnerable to these threats. Similarly, emergency planners in the United States—and increasingly elsewhere—now emphasize the dangers that are posed by catastrophic events, given our dependence on vital systems.

In what follows, we describe how these security experts have come to understand infrastructural dependence as an internal source of threat—and the techniques they have developed to mitigate this vulnerability. These expert practices work to make normally backgrounded aspects of infrastructure visible—not by observing its breakdown but by simulating its disruption. The claim of the chapter is not, then, that our polities are more vulnerable than they once were; rather, it is that system vulnerability has become a central problem structuring the way that technical artifacts are integrated into political calculation.

Critical Infrastructure Protection

Let us begin by describing current *critical infrastructure protection* (CIP) programs. CIP is a major aspect of homeland security strategy in the United States and has analogs in a number of European countries (see, e.g., Dunn 2005). Explicit governmental efforts to catalog critical infrastructure, assess its vulnerability, and mitigate threats to it began in 1996 with the Clinton administration's Presidential Commission on Critical Infrastructure Protection, which was formed in the wake of the Oklahoma City bombing and emerging concerns about the linkages created by information systems among technical infrastructures. U.S. security planners recognized that interoperability—the goal of much infrastructure development—was not only a boon to efficiency but also a potential source of danger; they argued that the interdependence of multiple infrastructures—information, communication, finance, energy—could lead to cascading and crippling failures.

After the attacks of September 11, CIP came to the center of homeland security strategy. The USA Patriot Act defined critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Department of Homeland Security [DHS] 2003, 6). In 2006 the Department of Homeland Security (DHS) released its long-delayed National Infrastructure Protection Program (NIPP), which contained an impressively long list of the sectors to be managed under the rubric of the nation's "critical infrastructures and key resources" (DHS 2006). These sectors included agriculture and food, the defense industrial base, energy, public health, banking and finance, drinking water and water treatment, chemical plants, dams, information technology, postal systems and shipping, transportation systems, and governmental facilities. This was the "stuff" that was to be made an explicit part of the new politics of security.

The NIPP contained three basic elements:

1. *Infrastructure inventory.* It sought to create a base of knowledge about the critical infrastructures of the United States in their complex interdependence by creating a "national infrastructure inventory." This inventory would gather "basic information on the relationships, dependencies, and interdependencies between various assets, systems, networks and functions" (DHS 2006, 31).
2. *Vulnerability assessment.* It called for the development of methods for analyzing risk that could guide resource allocation. These methods included vulnerability assessment—the identification of "intrinsic structural weaknesses, protective

measures, resiliency, and redundancies" in critical infrastructure (DHS 2006, 38).

3. *Coordination and federal assistance.* It defined the scope of federal intervention in CIP. The federal government was to play a coordinative role in the autonomous efforts of local governments and private sector actors and would distribute funds to state and local governments according to a "risk-based" formula to rationalize the expenditure of resources.

Thus the basic characteristics of critical infrastructure protection included, first, a concern with the critical systems on which modern society, economy, and polity depend; second, the identification of the vulnerabilities of these systems as matters of national security; and third, the development of security interventions whose aim is not to deter or defeat enemies but to mitigate system vulnerabilities.

Our goal here is not to evaluate whether such programs have in fact been successfully implemented (indeed, they have not) but rather to characterize their underlying logic. CIP is exemplary of a distinctive form of collective security, one that emphasizes protecting vital systems against potentially catastrophic threats. One of the key features of this form of security is that it seeks to manage the consequences of a variety of dangerous events—including terrorist attacks, natural disasters, and epidemics. It does this through the development and implementation of preparedness measures such as early warning systems, contingency planning, and scenario-based exercises.

As we have argued elsewhere, the genealogy of vital systems security can be traced to strategic bombing theory in interwar Europe, which focused on attacking the "vital, vulnerable" nodes of an enemy's industrial system (Collier and Lakoff 2007). This interest in the vulnerability of enemy systems was then internalized in U.S. programs for continental defense both before and during World War II. During the early cold war, U.S. civil defense planners were especially concerned to develop techniques to mitigate these vulnerabilities. Here it is useful to enter into some detail to see how the problem of system vulnerability has sparked the development of a novel security technology.

Vulnerability Mapping

The basic elements of this political technology of preparedness were developed during the early cold war, in response to the threat of a surprise attack by the Soviet Union. At this stage, preparedness meant massive military mobilization in peacetime to deter or respond to an anticipated enemy attack. The nation would have to be permanently ready for emergency, requiring ongoing crisis planning in economic, political, and military arenas. Civil defense was one aspect of such preparedness. U.S. civil defense plans were developed in response to the rise of novel forms of warfare in the mid-twentieth century: first, air attacks on major cities and industrial centers in World War II, and then intercontinental nuclear war. As World War II came to an end, U.S. military planners sought to ensure that the country did not demobilize after the war, as it had after World War I. They argued that the lack of a strong military had invited the surprise attack on Pearl Harbor. Now the Soviet Union presented a new existential threat. To meet it, the United States would have to remain in a state of permanent mobilization.

The U.S. Strategic Bombing Survey, conducted between 1944 and 1946, reported on the consequences of air attacks in England, Germany, and Japan and the effectiveness of these countries' civil defense measures. It recommended shelters and evacuation programs in the United States "to minimize the destructiveness of such attacks, and so organize the economic and administrative life of the Nation that no single or small group of attacks can paralyze the national organism" (Vale 1987, 58). The report pointed to the need to disperse key industries outside of dense urban areas and to ensure the continuity of government after attack. As Peter Galison has noted, the survey led military strategists to envision the United States in terms of its key weak points—to see the territory in terms of a set of targets whose destruction would hamper future war efforts (Galison 2001).

Faced with the threat of a surprise nuclear attack in the era of total war, military planners sought to develop a distributed system of preparedness that would enable civilian industrial production facilities to withstand an attack and support a viable counteroffensive (Collier and Lakoff 2007). Civil defense authorities in the 1950s created methods for spatially mapping domestic vulnerabilities to the threat of atomic warfare and then delegating preparedness activities to various agencies—from local government to individual families.

The prospect of a nuclear attack raised a number of interrelated questions for cold war national security planners: how would the enemy conceptualize U.S. national territory as a set of targets? What kinds of preparations were appropriate for meeting the threat of nuclear attack? And who should be responsible for organizing them? Civil defense authorities developed an elaborate set of planning practices. One of these was a procedure for mapping urban vulnerabilities. This procedure is significant in that it pointed toward the development of spatial knowledge about what would later be called critical infrastructure.

Vulnerability mapping generated a new form of knowledge about urban life. As opposed to statistical knowledge about the condition of the population, such as epidemiology or demography, this form of knowledge was not archival—it did not track the regular occurrence of predictable events over time; rather, vulnerability mapping produced knowledge about events—such as a surprise nuclear attack—whose probability could not be known but whose consequences could be catastrophic. Such knowledge involved not the calculation of probabilities but rather the imaginative enactment of events for which civil defense services would have to be prepared and the detailed analysis of how urban features would be affected by such events. In the process of evaluating vulnerability, planners made the material features of urban life an object of detailed political calculation.

Vulnerability mapping assembled a set of techniques for visualizing industrial facilities and population centers as targets of potential attack and developing appropriate response capabilities. This procedure not only meant identifying likely targets of attack; it also involved the imaginative enactment of attack to generate knowledge of which capabilities were needed to survive and fight back.

The 1950 document *United States Civil Defense* outlined the process of vulnerability mapping in schematic form (National Security Resources Board [NSRB] 1950). The starting point was the identification of "critical targets." To identify these targets meant developing a new way of understanding U.S. national space: through the reconstruction of the point of view of the enemy. Before the era of total war, knowing the mind-set of the enemy had been important mainly for planning theater operations. Now, the question was much broader: how did the enemy conceptualize U.S. territory as a set of targets?

United States Civil Defense assumed that the enemy would plan an attack based on the same principles of strategic bombing that were at the center of U.S. air-war doctrine. As the manual put it,

> The considerations which determine profitable targets are understood by potential enemies as well as our own planners. Such considerations include total population, density of population, concentration of important industries, location of communication and transportation centers, location of critical military facilities, and location of civil governments. (NSRB 1950, 8)

According to the civil defense plan, it was the job of each locality to determine its needs in preparing for attacks on critical targets within its jurisdiction. Planning at the local level was to be conducted through the imaginative enactment of a potential attack. Such an enactment would enable local civil defense planners to envision the probable impact of an attack, anticipate civil defense planning needs, and conduct exercises that would help identify weaknesses in their preparations.

United States Civil Defense provided a "hypothetical attack problem" as an example of how to identify civil defense needs. The hypothetical attack problem was a scenario consisting of an "attack narrative": it described two atomic detonations over an imaginary city *x:* one an air burst at twenty-four hundred feet and one an underwater burst (NSRB 1950, 117). The narrative then laid out the immediate impact of the attack: the water surge and lethal cloud of radioactive mist from the underwater burst; the explosive impact of the air burst and the flash fires that spread out up to a mile from ground zero; the casualties, including fourteen thousand to seventeen thousand from so-called mechanical injury (i.e., from the blast itself), seven thousand to eight thousand burn cases, and one thousand to three thousand radiation sickness cases from the air burst. The attack narrative also indicated the damage that would be inflicted on communications, transportation, utilities, and medical facilities.

All this information was intended to provide planners with knowledge of the exigencies for which they would have to prepare. "The hypothetical attack problem," argued *United States Civil Defense,* "should be realistic in order to bring out planning requirements in all segments of civil defense operations. The planners should accept the assumed effects, and analyze their needs accordingly" (NSRB 1950, 114). A city's civil defense needs could be determined as the difference between the envisioned impact of the bomb and its current response capabilities.

A series of technical manuals published by the Federal Civil Defense Authority gave local officials detailed instructions on how to make civil defense plans in a given city. For example, a 1953 manual titled *Civil Defense Urban Analysis,* guided planners in estimating how an atomic attack on a specific part of the city, at a specific time, would affect the structures and population of the city. The manual provided a detailed, systematic approach to mapping urban vulnerabilities. Knowledge of such vulnerabilities could then guide resources toward areas of greatest need.

This manual is of interest as a scheme for the development of a new knowledge of urban life as *tenuous*—in part because of its dependence on complex technological systems. Civil defense authorities saw that in the era of total war, the systems that had been developed to support modern urban life were now sources of vulnerability to enemy attack. Health facilities, systems of transportation and communication, and urban hygiene systems—whose construction had been essential to modern social welfare provision—were now understood in a new light, as possible targets and as necessary aspects of any emergency response. The material underpinnings of collective life were to be known and managed according to a certain political rationality.

The manual's introduction specified its aim and scope: "since the primary purpose of a civil defense urban analysis is to provide the tools for undertaking realistic civil defense planning, all pertinent aspects of the city must be considered" (Federal Civil Defense Administration [FCDA] 1953, 1). These pertinent aspects were to be considered in terms of their significance in the event of a nuclear attack. The relevant urban features to be analyzed were outlined in a lengthy table that constituted an impressive catalog of the elements of a city, including land use, building density, industrial plants, population distribution, police stations, the water distribution system, the electric power system, streets and highways, streetcars, port facilities, the telephone system, hospitals, zoos, penal institutions, underground openings (caves and mines), topography, and prevailing winds.

The table also indicated the "significance" of these features for civil defense planning. Thus knowledge about land use could help in estimating possible damage to various city functions. Industrial plants were significant as potential targets of sabotage or bombing and as important elements in police and fire-control planning. Water distribution systems were a potential target of sabotage and might be destroyed or disabled by a nuclear blast; they were also critical to fire control plans and were needed for emergency provision for attack victims and civil defense workers.

After identifying these features, planners were instructed to juxtapose them against one another on a series of operational maps. The goal of such maps was to determine which "pertinent" urban features would actually become important in the case of an attack and to present information that would be useful to specific urban services in formulating their civil defense plans. Once planners had assembled maps of significant urban features, the manual outlined a technical method for analyzing how these features would be affected by a nuclear attack. Given that the precise form of attack could not be known in advance, one needed a tool for modeling an attack's impact that was "sufficiently broad and flexible to meet all possible conditions" (FCDA 1953, 8).

To develop such a tool, the planner began by performing a "target analysis" to determine an enemy's assumed aiming point. The goal was to figure out what type of bomb a rational enemy would use to hit the city's main targets, and where the bomb would strike, to calculate the overall damage it would cause. To find the assumed aiming point, planners were to map both the area of industrial plant concentration and the distribution of the population. One then used a transparent acetate overlay with concentric circles indicating the level of bomb damage at different distances from ground zero. By placing the overlay on top of the map of facilities and population, the planner could estimate the point of attack that would cause maximum destruction. This was the assumed aiming point—which served as “a logical center for the pattern of civil defense ground organization of the community as a whole” (FCDA 1953, 10).

The next step was to estimate the damage a given sized bomb hitting a certain point would inflict. The technical manual focused this analysis on two key features of a city: first, facilities, such as industrial plants, public works, utilities, and services, and second, population. In each case, the point was not simply to measure the bomb’s impact (the number of buildings destroyed, the number of individuals killed, injured, or made homeless) but the city’s vulnerability—the relationship between blast impact and response capabilities.

In the case of structures, the factors determining damage were the size of the blast itself and possible damage from an ensuing firestorm. Physical damage from the blast was estimated by drawing concentric circles moving outward from ground zero, using information from a document that had been prepared by the Atomic Energy Commission and the U.S. Department of Defense (1950) called *The Effects of Atomic Weapons.* This document, based on data gathered in Hiroshima and Nagasaki, provided tables indicating blast damage from various bomb sizes at given distances from ground zero. Fire damage depended on such factors as building density, construction materials, precipitation, and wind velocity: here the key question was whether a blast would become a firestorm by spreading among neighboring buildings, which would obviously increase the structural damage considerably.

The manual directed planners to look at the destruction of facilities that would be important for response: “For example, one police station may house all of the police broadcasting equipment and one electric station may have the only available transformer which can change voltage from a distant source of electrical power to the voltage used for distribution through the city” (FCDA 1953, 53). The impact of an attack on the population, meanwhile, could be estimated as a function of the size and location of the bomb blast; the resident population versus daytime population in a given area (and therefore what time of day the bomb struck); and the condition of warning: was it a surprise attack or was the population on alert?

To map the city's probable number and distribution of casualties, the first step was to represent the distribution of the city's population in the city at the time of attack on a map based on estimates of daytime migration patterns. This was then paired with a table (provided by the federal authority) of the estimated percentage of fatalities and nonfatal injuries in a zone, given the size of the blast and the distance of the zone from ground zero. Using this table and an acetate overlay with concentric rings extending outward from ground zero, the planner would then "record the fatal casualties, nonfatal casualties and uninjured as calculated for each ring and for the various bomb sizes" (FCDA 1953, 36).

With this information, the planner could then generate isorithmic maps: city maps plotted with curving lines indicating the level of fatalities in a given subsector. These maps made it possible to visualize the distribution of casualties over the geography of the city. This tool for envisioning blast impact was a flexible instrument for assessing blast damage in generic terms at different points. Such maps brought urban populations into view as a spatially distributed set of casualty figures so that plans could be developed to provide relief in the wake of attack such as emergency medical and housing services.

The vulnerability mapping procedure thus provided a map of the physical damage of a likely blast, the casualties that resulted from it, and its impact on critical facilities. But more, it was characteristic of a way of coming to know national space—and the material features of that space—in terms of threat, vulnerability, and response capacity. This was not yet "critical infrastructure protection," but its basic logic was in place.

The Scenario

Over the course of the cold war, ambitious civil defense plans such as massive shelter systems were never fully implemented because of a lack of political will, skepticism about efficacy, and concern about their strategic implications. Nonetheless, a subset of security planners continued to attend to the problem of system vulnerability—still in relation to the threat of Soviet nuclear attack. Here it is illustrative to turn to the cold war trajectory of "imaginative enactment" as a knowledge production technique.

The practice of developing scenarios of nuclear attack to measure and improve current readiness was made famous by Herman Kahn of RAND in his 1962 book *On Thermonuclear War.* Kahn exemplified a new type of security expert distinctive to the period: not the military strategist or the civil defense planner but the "defense intellectual," a civilian with expertise in a technical domain—for example, mathematics, economics, or operations research—who applied this expertise to advise the government on nuclear strategy during the cold war.[3]

Kahn argued that for the strategy of deterrence to work, the enemy had to be convinced that the United States was prepared to engage in a full-scale nuclear war and had thus made concrete plans both for conducting such a war and for rebuilding in its aftermath. He criticized military planners for their failure to concretely envision how a nuclear war would unfold. If planners were serious about the strategy of deterrence, they had better be prepared to actually wage nuclear war. It was irresponsible not to think concretely about the consequences of such a war: what civil defense measures would lead to the loss of only fifty million rather than a hundred million lives? What would human life be like after a nuclear war? How could one plan for postwar reconstruction in a radiation-contaminated environment?

In the quest to be prepared for the eventuality of thermonuclear war, Kahn counseled, every possibility should be pursued. "With sufficient preparation," he wrote, "we actually will be able to survive and recuperate if deterrence fails" (Ghamari-Tabrizi 2005, 231). Kahn honed a method for what he called "thinking about the unthinkable" that would make such planning possible: scenario development. Like the civil defense attack narrative, Kahn's scenarios were not predictions or forecasts but opportunities for exercising an agile response capability. They trained leaders to deal with the unanticipated. "Imagination," Kahn wrote, "has always been one of the principal means for dealing in various ways with the future, and the scenario is simply one of the many devices useful in stimulating and disciplining the imagination" (Kahn 1962, 145).

Through the development of detailed attack scenarios, Kahn envisioned a range of postwar conditions whose scale of catastrophe was a function of prewar preparations, especially civil defense measures. These scenarios generated knowledge of infrastructural vulnerabilities and led Kahn to proposals for mitigating them. For example, a radioactive environment could hamper postwar reconstruction unless there was a way of determining individual levels of exposure. Thus he recommended giving out radioactivity dosimeters to the entire population in advance of war so that postwar survivors would be able to gauge their exposure levels and act accordingly.

All-Hazards Planning: Toward a Generic Technology

Let us now quickly summarize the process through which the methods of nuclear attack preparedness we have been describing became part of a more general political technology oriented toward multiple types of threat. Practices of civil defense were extended from nuclear attack to other types of disasters in the 1960s and 1970s through the advent of “all-hazards” planning. Beginning in the mid-1960s, state and local agencies—under the rubric of emergency management—sought to use federal civil defense resources to prepare for natural disasters such as hurricanes, floods, and earthquakes. Despite its different set of objects, the field of emergency management was structured by the underlying logic of civil defense: anticipatory mobilization for disaster. In the 1960s, state and local civil defense officials took up a number of the techniques associated with attack preparedness and applied them to natural disaster planning. These techniques included monitoring and alert systems, evacuation plans, training first responders, and holding drills to exercise the system.

Civil defense and emergency management shared a similar field of intervention—potential future catastrophes—which made their techniques transferable. Moreover, a complementary set of interests was at play in the migration of civil defense techniques to disaster planning. For local officials, federally funded civil defense programs presented an opportunity to support local response to natural disasters. From the federal vantage, given that civil defense against nuclear attack was politically unpopular, natural disaster planning developed capabilities that could also prove useful for attack preparedness. In the late 1960s, this dual-use strategy was officially endorsed at the federal level. Over the course of the 1970s, the forms of disaster to be addressed through emergency planning expanded to include environmental catastrophes, such as Love Canal and Three Mile Island, and humanitarian emergencies, such as the Cuban refugee crisis.

When the Federal Emergency Management Agency (FEMA) was founded in 1979, it consolidated federal emergency management and civil defense functions under the rubric of all-hazards planning. All-hazards planning assumed that, for the purposes of emergency preparedness, many kinds of catastrophes could be treated in the same way: earthquakes, floods, major industrial accidents, and enemy attacks were brought into the same operational space, given certain common characteristics. Needs such as early warning, the coordination of response by multiple agencies, public communication to assuage panic, and the efficient implementation of recovery processes were shared across these various sorts of disasters. Thus all-hazards planning focused not on assessing specific threats but on building capabilities that could function across multiple threat domains.

To operationalize all-hazards planning in the post-9/11 world, the DHS developed the National Incident Management System (NIMS). This is a system for deciding when a given event (an "incident of national significance," or INS) should trigger a temporary recomposition of governmental structures—and for governing how these temporary structures should operate. Multiple types of events can trigger the system: as the NIMS states, "For the purposes of this document, incidents can include acts of terrorism, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, typhoons, war-related disasters, etc." This final *et cetera* is worth emphasizing: it indicates the expansiveness of the category of the INS.

Contemporary Preparedness

The political technology of preparedness thus addresses a variety of events that threaten vital systems, including natural disasters, terrorist attacks, epidemics, and technological accidents. What these potential events have in common is that they are considered low-probability, high-consequence threats. It is not possible to gather knowledge about them based on archival records of their occurrence; nor can they necessarily be deterred or prevented. Security interventions must then anticipate their occurrence.

Here imaginative enactment as a way to generate knowledge about current needs in the face of future events remains a central tool. As an example, we can look at a 2004 Homeland Security Council document called *Planning Scenarios*. This was a set of fifteen disaster scenarios to be used by DHS as "the foundation for a risk-based approach" to homeland security planning. These possible events—including an anthrax attack, a flu pandemic, a nuclear detonation, and a major earthquake—were chosen on the basis of plausibility and catastrophic scale.

The scenarios were not predictions or forecasts; rather, they made it possible to generate knowledge of current vulnerabilities and the capabilities needed to mitigate them. As one expert commented, "we have a great sense of vulnerability, but no sense of what it takes to be prepared. These scenarios provide us with an opportunity to address that" (David Heyman, director of the homeland security program at the Center for Strategic and International Studies, quoted in Lipton 2005). Using the scenarios, DHS developed a menu of the "critical tasks" that would have to be performed in various kinds of major events; these tasks, in turn, were to be assigned to specific governmental and nongovernmental agencies.

Scenarios and scenario-based exercises are widely used in governmental and para-governmental preparedness efforts in the United States and elsewhere. They involve enactments of varying detail and scale, followed by reports on the performance of response. They are often designed by policy institutes and think tanks under contract to government agencies. In 2001, "Dark Winter" was performed, a scenario depicting a covert smallpox attack in the United States. This was an "executive-level simulation" set in the National Security Council over fourteen days. Current and former public officials played the roles of members of the National Security Council, and members of the executive and legislative branches were briefed on the results. One outcome was the Bush administration's decision to produce three hundred million doses of smallpox vaccine.

"Silent Vector" (2002) was an exercise in how to deal with the threat of an impending terrorist attack when there is not enough information to provide protection against the attack. The president, played by former senator Sam Nunn, was told of credible intelligence indicating an upcoming attack on the nation's energy infrastructure but was not given any information on where or when the attack would take place. Other examples include 2003's simulated anthrax attack, "Scarlet Cloud," "Black Dawn," which simulated a prospective al-Qaeda nuclear attack, held in Brussels in 2004, and the biennial TOPOFF exercises held by the DHS. TOPOFF 3 was enacted in April 2005 and included a car bombing, a chemical attack, and the release of an undisclosed biological agent in New Jersey and Connecticut. It was the largest terrorism drill ever, costing $16 million and including ten thousand participants. The event also included a simulated news organization, which was fully briefed on events as they unfolded.

In the January 2005 "Atlantic Storm," former secretary of state Madeleine Albright played the U.S. president in an exercise simulating a smallpox attack on multiple nations of the transatlantic community.[4] Istanbul, Frankfurt, Rotterdam, and multiple U.S. cities were hit. In a mock summit, former prime ministers of European countries played the role of heads of state. Questions of immediate response were posed: what kind of vaccination approach to use? Which countries have enough supplies of vaccine, and will they share them? Will quarantine be necessary? After the exercise, participants concluded that, first, there was insufficient awareness of the possibility and consequences of a bioterrorist attack; and second, no organization or structure is currently agile enough to respond to the challenges posed by such an attack. Structures of coordination and communication of response in real time must be put into place. The exercise produced a sense of vulnerability to new threats among participants.[5]

The conclusions were similar to those of other such exercises: governments are not adequately aware of or prepared for catastrophic events. Secretary of Homeland Security Michael Chertoff said of TOPOFF 3, "We expect failure because we are actually going to be seeking to push to failure" (DHS 2005). In producing system failure, scenario-based simulations generate knowledge of gaps in needed capability. These can then be the target of intervention. In so doing, they forge new links—communicational, informational—among various agencies: local and national government, public health, law enforcement, intelligence. These exercises are part of an effort to develop an integrated system for assigning priorities and allocating resources in preparation for emergency.

Thus the practice of linking possible future events to current vulnerabilities in vital systems is now widespread. Indeed, it is possible to map a growing field of "preparedness expertise" that develops this knowledge and makes recommendations for intervention. One might look, for example, at the work of the port security expert Stephen Flynn (2005), the public health expert Irwin Redlener (2006), or the natural disaster specialist Lee Clarke (2005)—or at reports produced by places like the RAND Center for Terrorism Risk Management Policy, for instance, the recent *Considering the Effects of a Catastrophic Terrorist Attack*. This report is based on a scenario in which terrorists conceal a ten-kiloton nuclear bomb in a shipping container and ship it to the Port of Long Beach, where the bomb explodes. While the report describes the massive death and destruction such a bomb might cause, it is mainly focused on the economic impact of this disruption of the global shipping supply chain. The report does not predict such an attack or calculate its likelihood. As the authors write, "We used this scenario because analysts consider it feasible, it is highly likely to have a catastrophic effect, and the target is both a key part of the US economic infrastructure and a critical global shipping center" (Meade and Molander 2006, xv).

We can make several points about this type of enactment. First, it is not a prediction, forecast, or model of how the future will unfold but rather an intervention in the present. Second, its purpose is not to provoke public anxiety or militate toward an intensified war on terror; rather, it is to generate expert knowledge about what the event would entail: as the RAND report states, it enables policy makers "to anticipate the types of decisions they might be called upon to make, reflect in time of relative calm on their options, and plan well in advance for contingencies" (Meade and Molander 2006, xviii). And third, it does not apply only to terrorism; the technique is also brought to bear to approach dangers such as avian flu, earthquakes and hurricanes, and environmental catastrophe. For example, the 2006 "Strong Angel" scenario exercise in San Diego combined an avian flu pandemic with a cyberattack, focusing on generating knowledge about how to design information systems for use by military and civilian organizations in humanitarian emergencies (Markoff

2006). And as is well known, FEMA had contracted a private firm to develop hurricane scenarios on the Gulf Coast prior to Hurricane Katrina—though DHS cut the program's budget so that the exercises were never conducted.

This leads us to a final point: failures of response do not undermine the norm of preparedness but rather intensify it—as we could see after Katrina, in political demands for better preparedness. This is characteristic of a political technology: it defines and regulates targets of intervention according to a normative rationality (see Rabinow 2003). In this case, the imagined enactment of events of a certain type—low probability, high consequence—makes it possible both to generate knowledge about vulnerabilities and develop techniques for mitigating them.

Conclusion

Techniques for generating infrastructural knowledge that were initially assembled as part of civil defense are now applied to planning for various types of disaster—hurricanes, floods, terrorist attacks, epidemics—and not only by the U.S. government. In conclusion, let us turn to the question of how attention to the ways that infrastructure is understood and managed by experts can be related to broader issues in the social theory of modernity.

Here it is useful to return to our earlier discussion of the work of Ulrich Beck on catastrophic risks. Beck argues that today, the very industrial and technical developments that were initially put in the service of guaranteeing human welfare now generate new threats. Our very dependence on critical infrastructures—systems of transportation, communications, energy, and so on—has become a source of vulnerability. For Beck, the danger emanating from technical developments such as nuclear accidents and genetically modified food shapes a more general perception that "uncontrollable risk is now irredeemable and deeply engineered into all the processes that sustain life in advanced societies" (Beck 2002, 39–56). Such dangers "abolish old pillars of risk calculus," outstripping our ability to calculate their probability or to insure ourselves against them.

As Francois Ewald points out, the precautionary principle has been an influential response to these novel forms of threat in Europe, especially those linked to the environment. In the context of possible catastrophe, Ewald notes, statistical calculation is no longer relevant—one must take into account not what is probable or improbable but what is most feared: "I must, out of precaution, imagine the worst possible" (Ewald 2002, 286). Thus a principle of precaution in the face of an incalculable threat enjoins against risk taking—for example, the implementation of new and uncertain technologies such as genetically modified food. In this manner, it seeks to keep the dangerous event from occurring.

In contrast, as we have described, a very different approach to uncertain but potentially catastrophic threats has emerged and extended its reach first in the United States and increasingly transnationally. Like precaution, it is applicable to events whose regular occurrence cannot be mapped through archival knowledge and whose probability therefore cannot be calculated. In contrast to precaution, however, this approach does not prescribe avoidance; rather, it enacts a vision of the dystopian future to develop a set of operational criteria for response. Preparedness does not seek to prevent the occurrence of a disastrous event but rather assumes that the event will happen. Instead of seeking to constrain action in the face of uncertainty, it turns potentially catastrophic threats into vulnerabilities to be mitigated. The technology of preparedness, as exemplified in programs such as critical infrastructure protection, thus brings a heterogeneous set of things into political reason. It is through this technology that experts and officials have come to see collective life as dependent on the functioning of a series of interdependent, complex, and above all highly vulnerable systems.

Notes

[1] This use of the term *political technology* follows the work of Michel Foucault, who showed that technical practices for managing life have been central to politics since the late eighteenth century, with the advent of biopolitics. Modern polities, he argued, are integrated not through a community of shared values along the model of the Greek *polis* but rather through a "political technology of individuals" (Foucault 1998).

[2] For critiques of the empirical validity of his claim that contemporary technological risks outstrip private insurability, see Bougen (2003) and Ericson and Doyle (2004).

[3] For Kahn's biography, see Ghamari-Tabrizi (2005).

[4] For a summary, see Smith et al. (2005).

[5] As a German official said, "For someone who has been around in the security and defense fields in its traditional sense for many years, this was quite a surprising and breathtaking exercise. . . . This is something I think a very small minority of politicians in Europe are aware of." See http://www.atlantic-storm.org/.

References

Barry, Andrew. 1999. *Political Machines: Governing a Technological Society.* London: Continuum.

Beck, Ulrich. 1999. *World Risk Society.* London: Wiley-Blackwell.

———. 2002. "The Terrorist Threat: World Risk Society Revisited." *Theory, Culture, and Society* 19, no. 4: 39–56.

Bougen, Phillip D. 2003. "Catastrophe Risk." *Economy and Society* 32, no. 2: 253–74.

Bowker, Geoffrey, and Susan Star. 1999. *Sorting Things Out: Classification and Its Consequences.* Cambridge, Mass.: MIT Press.

Clarke, Lee. 2005. *Worst-Cases: Terror and Catastrophe in the Popular Imagination.* Chicago: University of Chicago Press.

Collier, Stephen, and Andrew Lakoff. 2007. "Distributed Preparedness: The Spatial Logic of Domestic Security in the United States." *Environment and Planning D* 25: 7–28.

Department of Homeland Security. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Washington, D.C.: Department of Homeland Security.

———. 2005. "Transcript of Press Conference with Secretary of Homeland Security Michael Chertoff on the TOPOFF 3 Exercise." http://www.dhs.gov/xnews/releases/press_release_0650.shtm.

———. 2006. *National Infrastructure Protection Program.* Washington, D.C.: Department of Homeland Security.

Dunn, Myriam. 2005. "The Socio-political Dimensions of Critical Information Infrastructure Protection (CIIP)." *International Journal of Critical Infrastructures* 1, nos. 2–3: 258–268.

Edwards, Paul N. 2003. "Infrastructure and Modernity: Force, Time, and Social Organisation in the History of Sociotechnical Systems." In *Modernity and Technology*, ed. Thomas Misa, Philip Brey, and Andrew Feenberg, 185–225. Cambridge, Mass.: MIT Press.

Ericson, Richard V., and Aaron Doyle. 2004. "Catastrophe Risk, Insurance, and Terrorism." *Economy and Society* 33, no. 2: 135–73.

Ewald, Francois. 2002. "The Return of Descartes's Malicious Demon: An Outline of the Philosophy of Precaution." In *Embracing Risk: The Changing Culture of Insurance and Responsibility*, ed. Tom Baker and Jonathan Simon, 273–301. Chicago: University of Chicago Press.

Federal Civil Defense Administration. 1953. *Civil Defense Urban Analysis.* Washington, D.C.: Federal Civil Defense Administration.

Flynn, Stephen E. 2005. *America the Vulnerable: How Government Is Failing to Protect Us from Terrorism.* New York: HarperCollins.

Foucault, Michel. 2001. "The Political Technology of Individuals." In *The Essential Foucault,* vol. 3, ed. James Faubion, 403–417. New York: New Press.

———. 2007. *Security, Territory, Population: Lectures at the College de France.* New York: Palgrave.

Galison, Peter. 2001. "War against the Center." *Grey Room* 4: 6–33.

Ghamari-Tabrizi, Sharon. 2005. *The Worlds of Herman Kahn: The Intuitive Arts of Thermonuclear War.* Cambridge, Mass.: Harvard University Press.

Kahn, Herman. 1962. *Thinking About the Unthinkable*. New York: Horizon Press.

Lipton, Eric. 2005. "U.S. Report Lists Possibilities for Terrorist Attacks and Likely Toll." *New York Times*, March 16.

Markoff, John. 2006. "This Is Only a Drill: In California, Testing Technology in a Disaster Response." *New York Times,* August 28.

Meade, Charles, and Roger C. Molander. 2006. *Considering the Effects of a Catastrophic Terrorist Attack.* Washington, D.C.: RAND Center for Terrorism Risk Management Policy.

National Security Resources Board. 1950. *United States Civil Defense.* Washington, D.C.: National Security Resources Board.

Ong, Aiwa, and Stephen J. Collier. 2005. *Global Assemblages: Technology, Politics and Ethics as Anthropological Problems.* London: Blackwell.

Rabinow, Paul. 2003. *Anthropos Today: Forms of Modern Equipment.* Princeton, N.J.: Princeton University Press.

Redlener, Irwin. 2006. *Americans at Risk: Why We Are Not Prepared for*

Megadisasters and What We Can Do. New York: Random House.

Smith, Bradley T., Thomas V. Inglesby, Esther Brimmer, Luciana Borio, Crystal Franco, Gigi Kwik Gronvall, Bradley Kramer, Beth Maldin, Jennifer B. Nuzzo, Ari Schuler, Scott Stern, Donald A. Henderson, Randall J. Larsen, Daniel S. Hamilton, and Tara O'Toole. 2005. "Navigating the Storm: Report and Recommendations from the Atlantic Storm Exercise." *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 3, no. 3: 256–67.

U.S. Department of Defense. 1950. *The Effects of Atomic Weapons*. Los Alamos, N.M.: U.S. Atomic Energy Commission, Los Alamos Scientific Laboratory.

Vale, Lawrence J. 1987. *The Limits of Civil Defense in the U.S.A, Switzerland, Britain and the Soviet Union: The Evolution of Policies since 1945*. New York: St. Martin's.