Securing 'the Homeland'

Critical infrastructure, risk and (in)security

Edited by Myriam Dunn Cavelty and Kristian Søby Kristensen

2008

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

1 The vulnerability of vital systems

How 'critical infrastructure' became a security problem

Stephen J. Collier and Andrew Lakoff

In recent years, 'critical infrastructure protection' (CIP) has emerged as an increasingly important framework for understanding and mitigating threats to security. Widespread discussion of critical infrastructure protection in the US began in 1996, when President Clinton formed a Commission on Critical Infrastructure Protection. The Commission's 1997 report, *Critical Foundations*, established the central premise of infrastructure protection efforts: that the economic prosperity, military strength, and political vitality of the US all depend on the continuous functioning of the nation's critical infrastructures. As the report stated: 'Reliable and secure infrastructures are ... the foundation for creating the wealth of our nation and our quality of life as a people'. Moreover, the report continued, 'certain of our infrastructures are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security' (President's Commission on Critical Infrastructure Protection 1997: 3).

In discussions such as these, we find a distinctive approach to identifying, assessing, and managing security threats. The characteristics of this approach include:

1. a concern with the critical systems upon which modern society, economy, and polity are seen to depend;
2. the identification of the vulnerabilities of these systems and of the threats that might exploit these vulnerabilities as matters of national security;
3. the effort to develop techniques to mitigate system vulnerabilities.

In this chapter, we ask: where did this distinctive way of understanding and intervening in security threats come from? How did 'critical infrastructure' come to be regarded as a national security problem? We argue that critical infrastructure protection is best understood as one response to a relatively new *problematization* of security. As Foucault writes, a new problematization occurs when something has 'happened to introduce uncertainty, a loss of familiarity; that loss, that uncertainty is the result of difficulties in our previous way of understanding, acting, relating' (Foucault 1994: 598). As we will show, at pivotal moments in the twentieth century, technological and political developments rendered existing security frameworks inadequate, leading experts to

invent new ways of identifying and intervening in security threats. Specifically, what emerged was a way of understanding security threats as problems of *system vulnerability*. The task of protecting national security came to include ensuring the ongoing functioning of a number of vulnerable systems that were seen as vital to collective life.

The chapter follows a series of important moments in the twentieth-century history of system-vulnerability thinking: the interwar articulation of strategic bombing theory in Europe and the US, which focused on the 'vital targets' of an enemy's industrial system; the development of defence mobilization and emergency preparedness in the US during the Cold War as a means of defending the industrial system against a targeted nuclear attack; the emergence of all-hazards planning and 'total preparedness' as paradigms for response to disruptions of vital systems; and the widespread diffusion of formal models for assessing the vulnerability of vital systems (see Table 1).

The account culminates with discussions in the late 1970s and early 1980s among a relatively peripheral group of experts who were thinking about new challenges to national security. These experts had turned their attention to emerging threats – such as energy crises, major technological accidents, and terrorist attacks – that did not fit within the strategic framework of the Cold War. These new threats, they theorized, could not be deterred, and their probability could not be calculated. In this context, they began to draw together techniques and organizational forms developed earlier in the century to define a broad approach to mitigating the perceived vulnerabilities of the nation's critical systems. From their perspective, the ongoing functioning of such systems was a matter of national security. This approach to security problems was identified as central to post-Cold War national security in documents such as *Critical Foundations*, cited above.

Table 1 System-vulnerability thinking: 1918–present

	Key events	*Understanding of threat*	*Mitigation measures*
I. Total War and Strategic Bombing	Rise of airpower in the Second World War; Emergence of strategic bombing theory (post-Second World War); ACTS lectures (1930); AWPD-1 (1941)	Air warfare on vital targets/industrial web	Continental defence; early attack on enemy vital centres
II. Civil Defence	Strategic bombing survey; Soviet nuclear test (1949); Civil Defence Act (1950); Korean War	Soviet nuclear attack on critical target	Emergency response; vulnerability mapping; deterrence; second strike capacity
III. All-Hazards and System Vulnerability	1960s–1970s: rise of systems theory; emergency management (up to founding of FEMA in 1979)	All-hazards, nondeterrable, not predictable	Generalized contingency planning; generic system vulnerability analysis
IV. Systems Vulnerability as National Security Problem	Energy crisis and terrorism threat of 1970s through 9/11 and response	Vital systems vulnerability as national security problem	CIP

In describing the history of how infrastructure became a security problem, our analytic stance proposes neither that security threats are self-evident facts in the world nor that they are simply imagined. Rather, in studying problematizations, we are interested in how a given object – in this case, vulnerable, vital systems – becomes an object of expert reflection and practice. As Foucault writes:

> A problematization does not mean the representation of a pre-existent object nor the creation through discourse of an object that did not exist. It is the ensemble of discursive and non-discursive practices that make something enter into the play of true and false and constitute it as an object of thought (whether in the form of moral reflection, scientific knowledge, political analysis, etc).
>
> (Foucault 1994: 670)

The central figures in this story are mostly unknown planners and technicians in military and civilian bureaucracies who, over the course of the twentieth century, constituted system vulnerability as an object of thought. For the most part, their work has stayed below the surface of political debates about security. But the basic principles and practices they crafted can now be found in initiatives such as CIP. Our goal in tracing this history is to make this increasingly central approach to security problems available for critical scrutiny by analysing its elements and pointing to the contingent historical events and processes that shaped its formation.

Total war, strategic bombing, and the vital target

In this section, we trace the genealogy of system-vulnerability thinking to the rise of total war and the development of strategic bombing theory. The term 'total war' refers to a shift in the very constitution of war. In the nineteenth and early twentieth centuries, wars among major European powers were no longer conceived or conducted as battles between sovereigns. Rather, wars were fought between entire nations and peoples, bringing military and industrial organization into ever closer contact. As Aron (1954: 88) put it in a classic statement, the rise of total war meant that 'The army industrializes itself, industry militarizes itself, the army absorbs the nation; the nation models itself on the army'. In this

context, strategists increasingly recognized that military strength depended on the economic and social vitality of the nation, and on the state's capacity to mobilize and direct that vital strength to strategic ends.

The rise of total war meant that the traditional distinction between the military and civilian spheres – at least in wartime – was eroded in a variety of ways. In mobilizing for war, states vastly expanded their interventions in collective life. These interventions included controlling the production and distribution of industrial products critical to the conduct of war, particularly in sectors such as metallurgy and machine building, as well as the construction or regulation of electricity, transportation, and communication systems. These mobilization efforts had their counterpart in a new type of strategic thinking. Military strategists recognized that, just as their own economic facilities were critical to mobilization efforts, the vital nodes of enemy industrial systems could be exploited as vulnerabilities. An attack on these critical nodes could weaken or completely disable the opponent's war effort. Based on this line of reasoning, air power theorists developed a theory of air war – strategic bombing – in which such nodes constituted 'vital targets'.

Strategic bombing: enemy industrial facilities as targets

The Italian air power theorist Giulio Douhet is generally credited with first articulating the theory of strategic bombing. As Meilinger (1997: 8) points out, Douhet's approach was framed by the assumptions of total war. Douhet 'believed that wars were no longer fought between armies but between whole peoples. All the resources of a country – human, material, and psychological – would focus on the war effort'. The rise of total war had an important strategic consequence, according to Douhet: 'the *nation* would have to be exhausted before it would admit defeat'. The difficulty was that 'in an age of industrialization, when factories could produce the implements of war in a seemingly inexhaustible supply', the total defeat of a nation as a whole was an increasingly elusive goal, at least when pursued through conventional means (Meilinger 1997: 8). Douhet's contribution, in this context, was to provide a compelling (if not entirely prescient) vision of strategy in future wars.

Future warfare, Douhet argued, would not resemble the brutal defensive battles of attrition that had characterized the First World War. Rather, it would revolve around offensive actions, and particularly around offensive air power. The first task of strategic operations would be to achieve air dominance by disabling the enemy's air force and air defence. Once command of the air had been achieved, long-range bombers would be deployed to attack the nation itself. Specifically – and for our purposes, this is the crucial concept in Douhet's theory – these bombers would attack 'the most vital, most vulnerable, and least protected points of the enemy's territory' (cited in Meilinger 1997: 4–5). Douhet identified five vital centres of a modern nation that were the key targets of strategic bombing: industry, transportation infrastructure, communication nodes, government buildings, and 'the will of the people' (Meilinger 1997: 11).

Douhet did not substantially develop the theory of targeting beyond his general orientation to attack these vital targets. The most robust development of the theory of strategic bombing in the period between the wars took place in the US. In contrast to Douhet's strategy of using strategic bombing to break the will of an enemy people, the characteristic feature of the US school of strategic bombing was its emphasis on the critical target – the key node in an infrastructural or industrial system that, if destroyed, could bring an entire enemy war effort to a halt.

The most important centre for the development of US strategic bombing theory was the Air Corps Tactical School (ACTS). The ACTS also served as the training grounds for a large portion of the officer corps that applied the theory in developing US plans for air war in the Second World War (Faber 1997). ACTS theorists sought to identify the targets that were vital to a war effort, in particular through the development of the theory of the 'industrial web'. Billy Mitchell, an air power advocate whose ideas prefigured important dimensions of the industrial web theory, had written in 1927 that attacks on a few key nodes would mean that 'within a very short time the nation would have to capitulate or starve to death' (quoted in Greer 1985: 57). The writing and teaching of ACTS theorists echoed this approach. They argued that the complex interdependencies of modern economic systems were their essential weakness. ACTS graduate and, later, instructor Donald Wilson wrote in 1938 that the modern economy was composed of 'interrelated and entirely interdependent elements' (quoted in Faber 1997: 218). By attacking the 'essential arteries', or, in another pregnant metaphor, 'organic essentials' of a modern industrial structure, one could quickly – and economically – paralyse an enemy war effort (quoted in Faber 1997: 219).

One implication of this theory was that strategic bombing depended on detailed knowledge of the economic structure of the enemy nation. As ACTS theorist Muir S. Fairchild argued in 1938:

> Only by a careful analysis – by a painstaking investigation, will it be possible to select the line of action that will most efficiently and effectively accomplish our purpose, and provide the correct employment of the air force during war. It is a study for the economist – the statistician – the technical expert – rather than for the soldier.
>
> (quoted in Clodfelter 1997: 85)

The task of these experts would be to analyse the enemy's industrial systems – steel fabrication, transportation, finance, utilities, raw materials, and food supply – in order to select the 'relatively few objectives whose destruction would paralyze or neutralize' the enemy war effort (Greer 1985: 58).

This theory of strategic bombing profoundly influenced planning for the US air war in Germany and Japan during the Second World War. AWPD-1, the plan for air war against Germany, was based on intensive study of the German industrial system.[1] Beyond that, a clear line can be drawn from the theory of strategic

bombing to nuclear targeting strategy after the war (Freedman 1983). But the present discussion follows a different line of development. Just as air power theorists began to conceptualize the vital economic nodes of an enemy nation as a target of attack, they turned their strategic attention to the problem of an attack on the US. Their approach to analysing the vital nodes of an enemy's industrial system, initially developed as an air war strategy, was now transposed to a new understanding of the US as a space of vital and vulnerable targets.

The defence of vital systems: the US as target

For air power theorists, the development of strategic bombing as an offensive theory of attack on enemy vital targets raised the possibility of a similar attack on the US. Air power theorists assumed that the strategic orientation of a possible future enemy would be similar to their own. As a consequence, they began to envision the US – and in particular the critical systems of the US – as a target in a future war.

Continental defence

In the interwar period, military strategists engaged in an intense debate over the nature of air power and its role in a broader military organization. The question was: was air power primarily of tactical importance – to be deployed in support of ground operations? Or was there a separate strategic mission for air power that would justify an independent air force, and the development of long-range bombers? In the US, this dispute unfolded in discussions of continental defence. The long-standing assumption of US strategists had been that the central feature of US continental security was the presence of large oceans separating the US from potential enemies. Thus, traditionally, the Navy was assumed to bear primary responsibility for continental defence. Proponents of air power in the interwar period argued that the advent of long-range aircraft had changed the strategic situation dramatically. As another major ACTS figure, Lt. Kenneth Walker, put it:

> The importance assigned to Air Forces by major European powers, among which may be potential enemies, leaves no doubt our future enemies will unquestionably rely greatly, if not primarily, upon the actions of their Air Forces to bring about the defeat of the United States.
>
> (quoted in Faber 1997: 193)

Against long-range bombing, a model of continental defence based on naval power would be quickly rendered obsolete.

In making their argument for a new, air power-based approach to continental defence, ACTS theorists envisioned an air attack on the US by a coalition of European and Asian powers to illustrate the problems the military might face in a future war, given its current strategic assumptions and force structure. An ACTS theorist, Captain Robert Olds, laid out a scenario for a future war in testimony before the Federal Aviation Commission in 1935. One message of Olds' scenario (emphatically delivered with italics) concerned the necessity of creating an air force that was independent from other branches of the military. He argued that in a plausible war scenario, the existing air divisions of the US military – all of which were subordinated to the army and the Navy – would be drawn off to army or Navy engagements.

> A coalition of European and Asiatic powers have declared war on the United States. Superior naval forces ... seek a decisive naval engagement in the vicinity of the Panama Canal.... Such actions draw the U.S. Navy to Caribbean waters, *with its naval aviation*. Land forces from the Orient, using Alaska as an advanced base, seek ... to establish a salient in the area Washington, Oregon, California, and inland to about Salt Lake City, as a land base for further offensive operations in U.S. territory. The concentration of the U.S. Army *with its aviation*, in the western theater of operations would be mandatory to resist the land invasion.
>
> (quoted in Faber 1997: 194)

The implication of this scenario was that, given the existing force structure of the US military, the most vital targets of the US industrial system would be vulnerable to attack by the enemy air force.

> Simultaneously, the mass of the Allied [i.e., enemy] air forces have been flown, or shipped under submarine and patrol boat convoy, from Ireland to Newfoundland and are prepared to launch air attacks, from air bases in eastern Canada, against any targets of their choice in the vital industrial heart of our country.
>
> (quoted in Faber 1997: 194)[2]

The strategists at ACTS assumed that, following their own approach to strategic bombing, an enemy would attack the 'vital industrial heart' of the country. This meant, specifically, 'an industrial triangle extending from Portland, Maine, to the Chesapeake Bay to Chicago'. In this triangle lay '75% of all U.S. factories, almost all the nation's steelworks, most of its coal, and a number of major railroad centers, including New York, Washington, Pittsburgh, and Cleveland' (Faber 1997: 193). Attacks on the triangle would focus on rail lines, refineries, electric power, and water supply (Faber 1997: 194).[3] Following Douhet, the assumption was that an attack on these facilities might well destroy the American population's will to resist.

In anticipating such an attack, and in pressing their vision of the likely pattern of future war, ACTS theorists engaged in what was perhaps the first effort to catalogue the critical infrastructure of the US. In a lecture delivered in

1938 on 'National Economic Structure', Muir S. Fairchild declared that 'the key elements of American production were 11,842 "critical" factories, almost half of which were located in New York, Pennsylvania, and Massachusetts. The factories in those three states were "a concentrated objective which one might not suspect existed in this great continental industrialized nation of ours"'. Their destruction, or that of the transportation or power systems linking them, would 'apply tremendous pressure to our civilian population while at the same time seriously imparing [sic] our ability and capacity to wage war' (Faber 1997: 85).[4] The ACTS theorists, in short, were beginning to see the US as a collection of critical targets whose destruction would paralyse the economic system.

However, little action was taken in preparing the US for attack in the period before the Second World War. It was only during the course of the war, and really in its aftermath, that serious thought and organizational energy was given to the problem of organizing civil defence in the US.

Civil defence: mapping domestic vulnerability

Civil defence efforts in the US after the Second World War were, in a very direct sense, the defensive counterpart to strategic bombing doctrine, as the assumptions behind strategic bombing were transposed into a paradigm for the protection of vital systems against nuclear attack.[5] In the early years of the Cold War, planners developed techniques that made it possible to identify likely targets in the US, to model the effects of nuclear attack, and to anticipate requirements for emergency response.

The United States Strategic Bombing Survey, a massive effort to assess wartime bomb damage in Japan, Germany, and Britain, linked prewar strategic bombing and postwar civil defence.[6] The *Survey* took advantage of a rare opportunity to observe the effects of strategic bombing in practice. In doing so, it also necessarily assessed the civil defence efforts of these countries. One of the *Survey's* major findings was that civil defence had, in many cases, been effective in mitigating the effects of strategic bombing campaigns, and in maintaining an ongoing capacity to wage war in the face of attack. It concluded that a concerted national effort at civil defence was necessary, given the postwar threat the US faced from the Soviet Union. This finding led to a multi-year planning process that culminated in a 1950 report entitled *United States Civil Defense* (National Security Resources Board 1950)[7], which laid the groundwork for civil defence after the Second World War and for many aspects of emergency management in the US.

The approach articulated in *U.S. Civil Defense* was firmly situated in the assumptions of total war and of strategic bombing theory. 'The outcome of two world wars', it noted:

> has been decided by the weight of American industrial production in support of a determined fighting force. In any future war, it is probable that an enemy would attempt at the outset to destroy or cripple the production capacity of the US and to carry direct attack against civilian communities to disrupt support of the war effort.
>
> (National Security Resources Board 1950: 8)

U.S. Civil Defense assumed that a potential attacker would plan an attack based on the same principles of strategic bombing that were at the centre of US Air Force doctrine. As the report 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.
>
> (National Security Resources Board 1950: 8)

A number of questions followed from this argument: what would be the impact of attacks on these 'profitable targets'? What kinds of preparations would be appropriate to meeting this threat? And who should be responsible for organizing them? Elsewhere, we have argued that *U.S. Civil Defense* answered these questions by laying out a conceptual and organizational framework that we call 'distributed preparedness' (Collier and Lakoff 2008). Distributed preparedness delegated responsibility for civil defence functions to different levels of government, and to both public and private agencies, according to their competencies, capacities, and, of course, their spatial relationship to a likely target. Here, we focus on an aspect of distributed preparedness that is significant for the subsequent development of system-vulnerability thinking: a set of techniques we group together under the term 'vulnerability mapping'.

The purpose of vulnerability mapping was to gauge the potential impact of a nuclear attack on specific US cities, to assess how an attack would affect critical facilities, and to develop the capacities necessary to respond to such an attack. Vulnerability mapping enabled planners to understand cities and the systems that composed them as sites of potential future disaster and as complex landscapes of response. The basic technique was to create maps that visually juxtaposed an attack's projected impact against the existing infrastructure of an urban area. Using these maps, planners could assess weaknesses in existing response capacities and determine where resources would have to be directed in order to improve civil defence preparedness.[8]

The techniques used in vulnerability mapping deserve some elaboration. Three steps of the process are of particular relevance here:

1 cataloguing key elements of collective life in a target zone;
2 assessing the vulnerability of these elements to nuclear attack;
3 developing contingency plans that would mitigate these vulnerabilities.

In a first step, planners conducted an 'urban analysis' by creating an inventory of a given city's salient features for the purposes of civil defence. In various ways, these features could prove relevant to vulnerability in the event of an attack. Thus, for example, information about land use could help in estimating possible damage to urban facilities and in mapping the distribution of population – which was crucial to assessing likely casualties from a blast. Industrial plants were significant as possible targets of sabotage or bombing, and as important elements in police and fire-control planning.

The second step was to assess the vulnerability of the various elements in this inventory to a nuclear attack on a vital target. This assessment was conducted by juxtaposing a spatialized map of bomb damage over the existing features of a city. A transparent acetate overlay with regularly spaced concentric circles was placed on top of a map of industrial facilities and population concentrations. Each circle marked a zone in which the impact of a blast would be felt with a common intensity.[9] It was then possible to estimate the damage that a bomb of a given size, hitting a given point, would inflict on the significant features identified in the urban analysis.

The analysis of likely bomb damage made possible a third and final step, which was to use the estimate of the spatial distribution of physical damage and casualties over the existing structure of a city as a basis for emergency response plans. For example, information about damage to streets and highways, or general information about the spatial distribution of casualties, might be provided to engineering departments and 'incorporated in the general civil defense transportation map' (United States Federal Civil Defense Administration 1953: 53). Evacuation routes would thus be planned on the basis of the likely volume of evacuees over certain routes. What emerged from this analysis was a new understanding of cities in a nuclear age: as possible targets and as collections of vulnerable systems that had to be understood in their complex interrelationship.

A generalized approach to system vulnerability

The civil-defence approach to national vulnerability was initially designed for anticipating and organizing response to a Soviet nuclear attack. However, planners soon recognized that many of the assessment techniques and organizational forms developed to prepare for nuclear attack could also be useful in preparing for other types of threats, such as natural disasters. During the 1960s and early 1970s, techniques for analysing the vulnerability of systems and for planning response were generalized. This process was not the result of an overarching, explicit strategy, nor was it a central aspect of US national security thinking at the time. Rather, it took place through a series of autonomous developments that – as we show in the next section – were later brought together in a coherent framework as experts identified new problems of national security in the 1970s.

'Total preparedness' and all-hazards planning

As early as the 1948 Hopley Report, civil defence planners had suggested that the methods of nuclear attack preparedness could be extended to preparedness for other types of emergencies, such as natural disasters (Roberts 2006). In the 1950s and after, federal civil defence agencies were involved in disaster relief. For example, after Hurricane Diana struck the Northeast in 1955, the Federal Civil Defense Agency (FDCA) helped in coordinating assistance to states faced with disastrous flooding (Flemming 1957).

Nonetheless, for much of the Cold War period, preparations for disaster response remained secondary for federal civil defence agencies. Indeed, in the 1960s and early 1970s, federal officials were hesitant to allow state and local emergency management offices to use civil defence funds in preparation for natural disasters (Quarantelli 2000). Gradually, however, federal civil defence agencies began to accept the idea that organizing for nuclear attack and for natural disasters were complementary activities that drew on the same practices of vulnerability assessment and crisis management.

The practice of using civil defence resources for peacetime disasters was institutionalized by a 1976 amendment to the 1950 Federal Civil Defense Act. This shift was further advanced in the Defense Civil Preparedness Agency (DCPA) under President Carter.[10] The director of the DCPA co-authored a May 1977 statement summarizing discussions among federal, state, and local civil defence agencies, which acknowledged the legitimacy of using civil defence funds for natural disaster preparedness and defined a concept of 'total preparedness' that incorporated both civil defence measures and natural disaster preparedness: 'Local and State governments have the responsibility to provide preparedness for enemy attack as well as peacetime disasters. Therefore, DCPA's financial assistance to local and State governments may in the future be used to achieve *total preparedness against any risk*' (Joint Committee on Defense Production 1977: Appendix A, 38). All-hazards planning became official policy at the federal level with the establishment of the Federal Emergency Management Agency (FEMA) in 1979 (for a summary of key organizations in this story, see Figure 1).

The shift to 'total preparedness' can also be observed in the area of defence mobilization. During the Cold War mobilization that began in 1950, a series of governmental agencies had the task of ensuring that a productive and logistical network was in place to support a US war effort. In doing so, these agencies – some of which were part of civil defence programmes, some of which were in military branches – were also concerned about the condition of this production and distribution network after a nuclear attack. The Office of Defense Mobilization in the Executive Office of the President (1950–8) was one site for such preparedness planning.

As in emergency response, the organizations involved in defence mobilization – whose official task was to assure the nation's industrial capacity for war-fighting – were, nearly from their inception, also involved in planning for

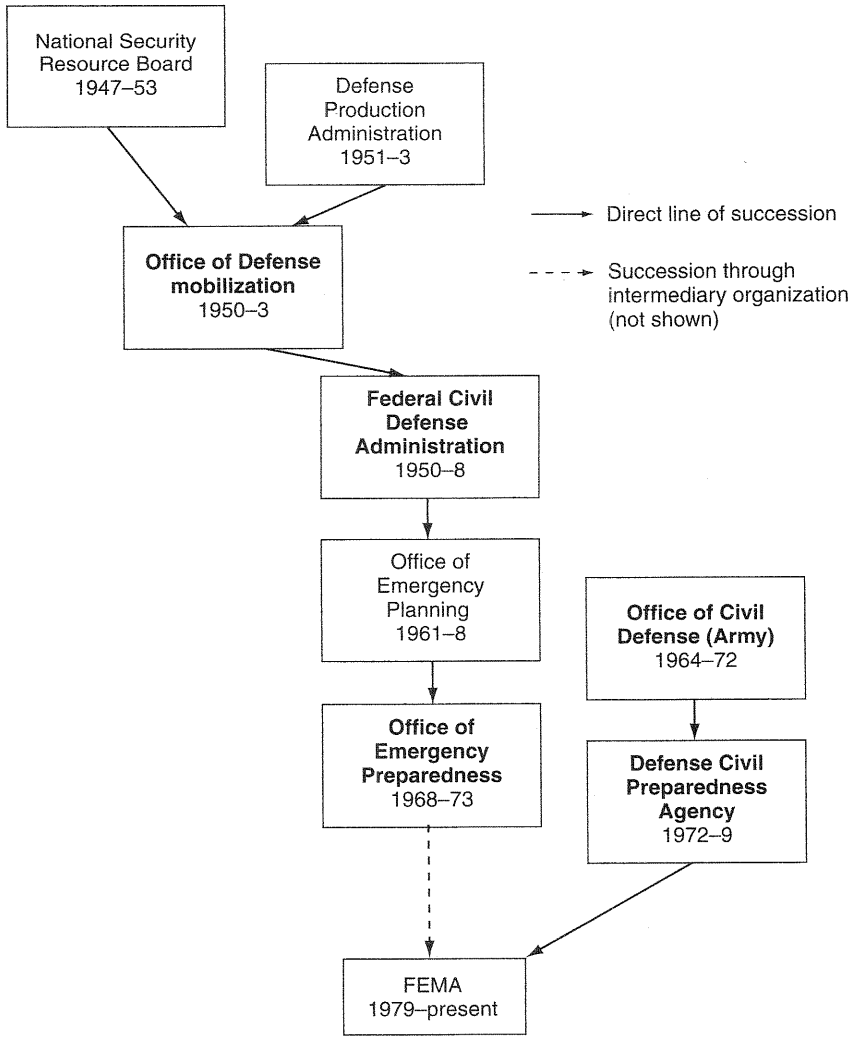

Figure 1 Organizations involved in US Emergency Response and Defense Mobilization (organizations mentioned in text indicated bold face).

other types of threat. For example, in the mid-1950s, the Office of Defense Mobilization explored the possibility of adapting its nuclear attack damage-assessment procedures to natural disasters. A devastating 1955 flood in California provided the occasion for one such experiment. However, as was the case with civilian emergency response in the 1950s, the main emphasis in defence mobilization remained on war readiness. Civil defence planners saw preparedness for natural disasters as an opportunity to test techniques and train personnel for the cataclysmic event of a nuclear war (Flemming 1957).

Over time, defence mobilization officials shifted toward a total preparedness approach. In part, they did so to convince the managers of private sector utilities – who were convinced of the need for natural disaster preparedness, but reluctant to engage in nuclear preparedness – to voluntarily implement safeguards against nuclear attack. For example, a 1970 manual for oil refineries published by the Interior Department and the Army Office of Civil Defense encouraged managers in charge of safety and reliability to plan not only for typical contingencies like fires or accidents, but to simultaneously prepare for a nuclear bomb blast. The argument from the manual was that the two forms of planning were complementary – and essential to national security in a broad sense.

> Since the petroleum industry including natural gas has the responsibility of supplying over 75% of the energy for our economy, the country must have petroleum processing facilities of adequate strength and management ready to cope with *all emergencies be they of natural origin or doings of mankind.*
> (Stephens 1970: v, emphasis added)

Civil defence planners thus developed a generic notion of 'emergency' that would enable them to take advantage both of local government capacities and private sector activities in the service of total preparedness.

System vulnerability and crisis management

The shift to total preparedness involved not only the kinds of institutional changes described above, but also a number of technical developments. Technicians involved in emergency planning used systems analysis to develop formal models of vulnerability. These models did not assess the impact of specific events, but rather analysed the *intrinsic vulnerability of systems* to disruptions of any kind. The use of such methods was part of the broad diffusion of operations research and systems analysis methods across US government bureaucracies during the 1960s (Jardini 2000; Amadae 2003; Light 2003).

An example of such efforts can be found in the sphere of defence mobilization – specifically, electricity sector preparedness. The Defense Electric Power Administration (DEPA) had been formed in the early 1950s as part of the broader remobilization that began with the onset of the Korean War. Like other defence mobilization agencies created at the time, its aims were both to assure adequate development of power resources for defence production and to prepare for dealing with the damage that production and transmission facilities would suffer in the event of a nuclear attack. In the early 1960s, this agency was calculating the likely effects of a nuclear blast largely by employing the techniques developed in early civil defence described above, which involved estimating the impact of a nuclear attack on a critical target. Toward the end of the 1960s, however, DEPA studies began to adopt formal techniques – such as linear programming – that changed the approach to vulnerability assessment. The shift was from the analysis of specific events to generic models of system vulnerability. As

a group of experts in the field wrote in a 1975 report to the Defense Civil Preparedness Agency, 'vulnerability evaluations of electric power systems have progressed from detailed, specific analyses of particular systems reacting to a specific nuclear attack to general methods of evaluation using sophisticated modeling techniques' (Lambert and Minor 1973).

These techniques made it possible to assess the impact of a potential disruption not only on electrical production and distribution, but also on 'secondary' systems – industrial enterprises, for example. This progression was consistent with a shift to an all-hazards approach, but added a specific focus on the intrinsic vulnerability of systems, and a methodology for assessing the interdependencies among systems, to the toolkit. What was novel were the methods of technical analysis: whereas prewar 'industrial web' theorists had been concerned with interdependency and the effect of disruptions on interconnected structures, they did not have a quantitative method for analysing these interdependencies.

By the late 1960s, systems analysis was being employed in other areas of civil defence, such as the White House Office of Emergency Preparedness (OEP). The OEP was a successor to the Office of Defense Mobilization, but its purview was broader. Its mission was to ensure that the government would respond effectively to various types of emergency. The OEP was charged with coordinating response to multiple types of crisis over the course of the early 1970s, including the wage-price freeze of 1970, a threatened Penn Central Railway strike, and the Emergency Petroleum Allocation Act of 1973.

A department within OEP, called the Systems Evaluation Division (SED), was devoted to the formal analysis of critical systems – such as transportation, energy, and communication – as part of a broad vision of crisis management. A major figure in SED was Robert H. Kupperman, a specialist in operations research who had come to OEP from the Institute for Defense Analysis (IDA), a civilian think-tank that conducted technical research for the Defense Department. Kupperman would later participate in discussions about the formulation of critical infrastructure protection programmes in the US, such as the expert panel for *Critical Foundations*. In SED, he initially focused on producing a sophisticated mathematical analysis of the strategic implications of anti-ballistic missile systems (Kupperman and Smith 1972; Hiltz and Turoff 1978). In subsequent work, he applied the tools of systems analysis to the problem of system vulnerability. For example, he led a detailed analysis of the role conservation measures could play in averting an anticipated energy crisis – as well as the economic impact of such measures. This work analysed patterns of energy consumption in multiple sectors, including electricity, transportation, and industrial production.[11]

Through his work in SED, Kupperman became interested in the common structure of response to crisis situations. What was crucial across all of them, he argued, was the need to have crisis management techniques in place *before* the advent of the crisis. In this sense, his work was structurally similar to the all-hazards approach in emergency management. In a 1975 article on crisis management and computer-based communication, Kupperman and his co-authors pointed to characteristics shared by diverse types of crisis – including hurricanes, terrorism, and famine. The authors wrote that in order to adequately respond to such events, which were increasing in number and complexity, coherent systems of preparedness planning must already be in place: 'As we begin to recognize the complex problems that threaten every nation with disaster', Kupperman asked, 'can we continue to trust the ad hoc processes of instant reaction to muddle through?' (Kupperman *et al.* 1975).

System vulnerability as a national security problem

Up until the mid-1970s, these various initiatives in emergency management, civil defence, and defence mobilization were not organized around a single national security framework. Part of the reason was organizational dispersion: they were spread out among various agencies engaged in specific activities such as crisis management. It was also due to the peripheral status of civil defence thinking during the Cold War. Throughout most of the Cold War, civil defence was a fairly marginal aspect of national security debates, which were focused on strategies for deterring the Soviet threat. From the vantage of the dominant strategic paradigm – mutually assured destruction – civil defence was dangerously destabilizing, since it presumed that one could fight and win a nuclear war.[12]

Beginning around the mid-1970s, however, some security experts began to re-conceptualize the objects and aims of national security, particularly in response to events such as terrorist attacks and the energy crisis. They argued that these events presented new national security challenges – which could not be adequately approached within the Cold War strategic paradigm. In this context, one subgroup of experts sought to apply practices that had been developed in areas such as emergency management and defence mobilization to a novel set of threats.

Non-deterrable threats

In the 1970s, a subgroup of security thinkers with ties to civil defence – including Kupperman and his colleagues – became concerned with the rise of threats other than the Soviet Union. Events such as the 1972 Munich terrorist attacks, followed soon after by the Arab–Israeli War and the 1973 oil crisis, indicated to these thinkers that the nation's dependence on critical systems was a vulnerability that could be exploited by actors who lacked the military strength to directly challenge the US.

As we have seen, in OEP, Kupperman was concerned with anticipating and managing potential future energy crises. After the events of the early 1970s, he linked this concern to the problem of terrorism. He argued that terrorism was emerging as a strategic tool in low-intensity conflict – and that terrorists were likely to exploit vulnerabilities in the nation's critical systems (Kupperman *et al.* 1982: 463). This emphasis on the conjuncture of terrorism and the vulnerability of energy systems was shared by other civil defence-oriented security thinkers, such as Maynard M. Stephens, the author of the 1970 study on oil refineries

cited above. In a 1979 volume on terrorism co-edited by Kupperman, Stephens wrote that 'the uninterrupted flow of natural gas is economically essential to the country' (Stephens 1979: 213). For this reason, he argued, 'segments of major natural-gas transmission lines should therefore stand out as attractive targets to the saboteur' (Stephens 1979: 213).

Such arguments followed the concern, first developed in strategic bombing theory with critical nodes of a production system that, if disrupted, could knock out an entire industrial web. There was a crucial difference, however. The threat now came not from an enemy's military attack, but from non-deterrable threats – terrorism, and 'threats without enemies' such as technological failures and natural disasters. In short, total preparedness was no longer viewed as an adjunct to the problem of confronting the Soviet Union. Rather, it was seen as a national security problem in its own right.

This elevation of systems vulnerability to the level of a national security concern had a certain political salience in the period, given the contemporary concern with problems such as energy and terrorism. For example, in 1977, the Joint Congressional Committee on Defense Production held hearings and published a two-part report on the nation's 'civil preparedness' programmes. The report was highly critical of the condition of the nation's emergency management plans. It recommended the centralization of federal preparedness efforts and a broadening of these efforts to include non-nuclear threats. The first volume of the report articulated, in now-familiar terms, two key aspects of the vital systems security framework: the dependence of contemporary society on complex technological systems, and the vulnerability of citizens to multiple types of threat. 'An increasingly complex, technology-dependent, industrial economy in the United States', the report argued, 'has made citizens more than ever vulnerable to the effects of disasters and emergencies over which they have little or no control and to which they cannot successfully respond as individuals' (Joint Committee on Defense Production 1977: 3). Moreover, the report noted 'increasing demands made on government by citizens' for protection against such threats'.[13]

In July 1977, soon after the Committee's *Civil Preparedness Review* was published, a major blackout occurred in New York City. The blackout, which was accompanied by extensive riots and looting, brought widespread attention to the frailty and vulnerability of the nation's electrical grid and other critical systems. The Defense Production Committee held hearings shortly after the blackout on the implications of the event for federal emergency preparedness. One conclusion was that these systems were vulnerable to a wide array of threats, ranging from technical accidents to natural hazards and terrorist attacks: 'Electric utilities therefore present a relatively compact and especially inviting set of targets for a saboteur, a terrorist or an attacker, as well as a lightning bolt' (Joint Committee on Defense Production 1977: 1f.). The problem of system vulnerability was projected onto the enemy's strategy, in a mirroring process that was similar to early civil defence.

At these hearings, the director of the Defense Logistics Agency testified about military efforts to protect key defence industries from attack. He noted that the scope of his agency's activity was limited to those industries that had a direct impact on defence needs. Considering the widespread impact of the New York City blackout on economic and social life, he suggested the need for a broader programme to secure critical facilities. This would begin with a cataloguing effort:

> It might be well if there were some sort of national list, if you please, of facilities that would be a key to our economic and societal well-being. Then at least, we would know what they are and whether or not the Federal Government would see fit to involve itself in providing for their security or would provide at least some advice on what these facilities could do for themselves.
>
> (Joint Committee on Defense Production 1977: 117)

What is significant in these recommendations is the proposal that the federal government should generalize its efforts to assure critical infrastructure, from a specific emphasis on those systems essential to military production to a broader concern with the vital systems essential to the economic and social well-being of the nation as a whole.

A mature paradigm

In 1984, the Center for Strategic and International Studies (CSIS) at Georgetown published a report, called *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks* (Woolsey *et al.* 1984). The report was based on the work of a 'Panel on Crisis Management' chaired by Kupperman and R. James Woolsey. It can be seen as a fully articulated vision of system-vulnerability thinking as a distinctive approach to national security. Its producers were marginal to governmental policy at the time. However, this vision would come to the centre of policy discussions a decade later in the Clinton administration with the explicit articulation of 'critical infrastructure protection' as a national security problem.

The CSIS document synthesized the basic elements of system-vulnerability thinking whose development we have tracked so far: it identified the protection of vital systems as a question of national security; it argued that these systems were vulnerable to threats that could not be deterred, and whose risk could not be assessed through probabilistic analysis; it proposed a framework of preparedness that included a range of techniques for mitigating vulnerabilities, including ways of understanding systems (cataloguing, vulnerability assessment), measures to secure these systems; and plans for response to their disruption. But it went one step further, proposing that system vulnerability be seen as an autonomous problem of national security in a post-Cold War world, one that was distinct from the threat of foreign enemies. The elements of 'critical infrastructure protection' discussed at the outset of this chapter were now in place.

Security problem: the protection of vulnerable, vital systems

The report argued that the nation had become economically, technologically, and psychologically dependent on a number of 'highly complex service networks' for 'our daily well-being' (Woolsey *et al.* 1984: 4). It emphasized the risk to national security posed by the fragility and interdependency of these systems: 'We live in a civilization at risk, as much from the increasing fragility and brittleness of its technological fabric as from the more visible and apparently urgent threats from abroad'. The report enumerated the qualities of critical systems that made them both an efficient means of distribution and a source of vulnerability: they are made up of multiple nodes and are interconnected by links that facilitate the circulation of goods and information (Woolsey *et al.* 1984: 11). It was not in principle difficult to disrupt the operations of these networks, given their interdependence: 'denial of the essential resources – human, energy, and fiscal – that make networks function will quickly bring their operations to a halt'.

Threats to vital systems as national security problems

The disasters that threaten these systems, the report argued, were not regularly occurring events, such as those mitigated by insurance; nor were they rational enemies that could be managed through strategies such as diplomacy and deterrence. Rather, the threat consisted of low-probability, high-consequence events. These included terrorists or dissidents who had the capacity and intention to do harm. But other kinds of events, such as natural disasters or technological accidents, could also severely disrupt critical systems, according to the report. The potentially catastrophic effects of such events meant that they had to be planned for even if they were rare or improbable: 'This is an explosive combination that serious and responsible national leaders need to address, however low a probability one might reasonably assign to any particular network vulnerability being exploited at any one time' (Woolsey *et al.* 1984: 7).

Techniques for mitigating vulnerabilities: contingency planning, preparedness

Given that such events could not be predicted, or necessarily prevented, the emphasis in the report was on reducing the vulnerabilities of critical systems. Since these networks were interrelated and interdependent, the report argued, a comprehensive programme of protection must be developed. The report introduced a number of measures for ensuring the continued functioning of critical systems in the event of emergency, most of which had evolved over the years in emergency response and defence mobilization programmes: improving system resilience, building in redundancy, stockpiling spare parts, performing risk analysis as a means of prioritizing resource allocation, and running scenario-based exercises in order to test readiness. A final key element in the report's broad 'philosophy of crisis management' was the specification of responsibilities in the event of emergency – who would make preparations, who would declare a state of emergency, and who would be in charge during the actual emergency. While these recommendations were not directly implemented, the CSIS report is significant for our story in that it exemplifies the process through which systems vulnerability as a problem came to the centre of national security strategy.

Conclusion: vital systems security

In this chapter we have described the process through which a new way of defining and intervening in collective security problems emerged over the course of the twentieth century. Through this process, experts began to define a new class of threats to security: events that threatened the vital systems supporting collective life. In conclusion, we consider how this new way of approaching security problems relates to the notion of 'critical infrastructure protection' as it emerged in the last decade.

CIP as a concept and practice was first explicitly articulated in the 1990s. As Myriam Dunn Cavelty argues (Chapter 2, this volume), early CIP policy focused on cyber-infrastructures, responding to a growing concern regarding information security that had developed in the US government during the 1980s. Experts then expanded the concept to include the entire range of critical infrastructures on which economic and political life were seen to depend. After the attacks of September 11, CIP moved to the centre of domestic security doctrine. The story we have told in this chapter suggests that this development is not best understood as a process of the 'securitization' of a civilian sector. Rather, it would be better to say that in the 1980s and 1990s, a growing concern about information security found a technical vocabulary, a set of analytical tools, and practices of intervention in a long-standing mode of thinking about infrastructures as a security problem.

Although it has not been the focus of this chapter, it would certainly be possible to trace the lines of connection between the history we have recounted and the explicit articulation of critical infrastructure protection in the 1990s. Thus, for example, both Kupperman and Woolsey participated in an expert panel as part of a 1997 Institute for Defense Analysis (IDA) report to the President's Commission on Critical Infrastructure Protection (Institute for Defense Analysis 1997). Furthermore, a remarkable proportion of the support staff for the pivotal *Critical Foundations* report were officers in the Air Force (President's Commission on Critical Infrastructure Protection 1997: iv). More broadly, critical infrastructure protection has clear conceptual connections and institutional precursors going all the way back to strategic bombing theory. Seen against the background of the history of system-vulnerability thinking in the twentieth century, the underlying rationality of critical infrastructure protection is entirely familiar.

Notwithstanding these continuities, the emergence of CIP as an explicit area of government initiative does, we argue, mark an important development in the

history of system-vulnerability thinking. For most of the twentieth century, the elements of system vulnerability we have described – 'vulnerability analysis', 'contingency planning', and so on – functioned as adjuncts to a paradigm of sovereign state security that was concerned with defence against foreign threats. As we have shown, in the interwar period and the Cold War, the rudiments of system-vulnerability thinking were developed as specific responses to the challenges posed by the threat of air war or Soviet nuclear attack. We might say that in these contexts system-vulnerability thinking – as a way of conceptualizing security problems and intervening in them – was circumscribed and limited by the exigencies of sovereign state security.

This situation began to change as the major existential threat of the postwar period – Soviet nuclear attack – faded, and new threats such as terrorism, technological failure, and energy crises came to be identified as central to national security. The identification of these threats introduced, in Foucault's language, an 'uncertainty' provoked by difficulties in 'previous way[s] of understanding, acting, relating'. It was unclear whether the questions and concepts of sovereign state security could be meaningfully applied to these new risks. In this context, techniques for understanding and managing system vulnerability were disarticulated from the specific demands of sovereign state security. The mitigation of system vulnerability came to be seen as an autonomous aim of security policy. In the process, national security came to be defined, at least in part, in terms of the security of vital systems (Collier and Lakoff 2006).

It is important to bear in mind that this new way of understanding security problems has not, thus far, produced stable organizational forms or modalities of intervention. For the moment, rather, what we observe is a profusion of plans, schemas, techniques, and organizational initiatives that respond to new kinds of perceived threats to collective security. Critical infrastructure protection is only one such response, and one whose actualization in bureaucratic arrangements, resource flows, and established regimes of security is just beginning to emerge.

Notes

1 The wartime bombing effort also led to the development of optimization techniques (in systems analysis and operations research) that, as we see below, were to prove important in formalizing understandings of system vulnerability in the 1960s and 1970s.
2 According to Greer (1985), this scenario of a European coalition combined with an Asian power was the common assumption used in US military planning before the Second World War.
3 This enumeration of likely targets within the 'industrial triangle' was laid out by Captain Harold Lee George, another major figure in ACTS, at the same hearings.
4 Fairchild's words, quoted by Faber (1997: 85), are in single quotation marks. ACTS theorists worked extensively with examples from the US for reasons other than a concern with continental defense. Extensive information about the industrial structure of other countries was not available, and taking examples that assumed bombing of potential future adversaries by the US military was considered provocative.
5 Civil defense was not the only response to this new awareness of the US as a target. A range of policies were taken to reduce the vulnerability of industries that would be essential to war production, including the promotion of industrial dispersion, discussed in Galison (2001) and Light (2002), and programmes to assure that the US had enough redundant capacity to manage disruptions of industry due to strikes.
6 McMullen (2001) discusses the relationship of the *Strategic Bombing Survey* to the transformation in Air Force doctrine. Key figures from the ACTS, including Muir S. Fairchild, played central roles in the *Survey* (Faber 1997).
7 *U.S. Civil Defense* led to the 1951 Civil Defense Act – which in turn created the Federal Civil Defense Administration. Lee (2001: 60) argues that *U.S. Civil Defense* – referred to as 'The Blue Book' – served 'as the blueprint for structuring the Federal Civil Defense administration'. More broadly, the document laid out a new model that would subsequently be adopted in a range of other contexts for managing 'emergency' situations. For a review of the studies that led up to *USCD*, see Lee's chapter 'Careful studies and indecision'.
8 This discussion draws in particular on a document titled *Civil Defense Urban Analysis* (United States Federal Civil Defense Administration 1953).
9 Damage from the blast in each zone could be estimated using information from a document that had been prepared by the Atomic Energy Commission and the Department of Defense, called *The Effects of Atomic Weapons* (United States Department of Defense, Los Alamos Scientific Laboratory 1950). This document, based on data gathered in Hiroshima and Nagasaki, provided tables indicating blast damage from a nuclear strike at various distances from ground zero.
10 In testimony to the Joint Committee on Defense Production, the director of Civil Preparedness (who had been appointed in April 1977) noted:

> The previous Administration sought to limit civil defense support of State and local government to preparations for nuclear attack only. This position was rejected by the Congress in P.L. 94–361 and by this Administration under my recently announced policy of dual use preparedness.
>
> (Joint Committee on Defense Production 1977: 35)

11 This work is summarized by the head of the Office of Emergency Management, George A. Lincoln (Lincoln 1973).
12 Patrick Roberts writes that in 1970s, 'civil defense advocates tussled with proponents of mutually assured destruction, who believed that civil defense efforts were futile since the whole point of deterrence was to convince both sides that there could be no winner in a nuclear war' (Roberts 2006: 60).
13 The growth in the significance of the word preparedness, although little remarked, has resulted primarily from two factors: (1) the increasing vulnerability of a complex, highly interdependent industrial society, and (2) the increasing demands made on Government by citizens whose lives may be dramatically affected by a range of emergencies they are unable to prevent or control.
(Joint Committee on Defense Production 1977: 3)

References

Amadae, S.M. (2003) *Rationalizing Capitalist Democracy: The Cold War Origins of Rational Choice Liberalism*, Chicago: University of Chicago Press.

Aron, R. (1954) *The Century of Total War*, Garden City: Doubleday.

Clodfelter, M.A. (1997) 'Molding airpower convictions: Development and legacy of William Mitchell's strategic thought', in Meilinger, P.S. (ed.) *The Paths of Heaven: The Evolution of Airpower Theory*, Maxwell Air Force Base: Air University Press, pp. 79–114.

Collier, S.J. and Lakoff, A. (2006) *Vital Systems Security*, ARC Working Paper no. 2, Berkeley: Anthropology of the Contemporary Research Collaboratory.

Collier, S.J. and Lakoff, A. (2008) 'Distributed preparedness: space, security and citizenship in the United States', *Environment and Planning D: Society and Space*, 26, 1: 7–28.

Faber, P.R. (1997) 'Interwar US army aviation and the Air Corps Tactical School: incubators of American airpower', in Meilinger, P.S. (ed.) *The Paths of Heaven: The Evolution of Airpower Theory*, Maxwell Air Force Base: Air University Press, pp. 183–238.

Flemming, A.S. (1957) 'The impact of disasters on readiness for war', *Annals of the American Academy of Political and Social Science*, 309: 65–70.

Foucault, M. (1994) *Dits et Ecrits, 1954–1988*, Paris: Gallimard.

Freedman, L. (1983) *The Evolution of Nuclear Strategy*, New York: St. Martin's Press.

Galison, P. (2001) 'War against the center', *Grey Room*, 4, Summer: 6–33.

Greer, T.H. (1985) *The Development of Air Doctrine in the Army Air Arm, 1917–1941*, Washington, DC: Office of Air Force History, U.S. Air Force.

Hiltz, S.R. and Turoff, M. (1978) *The Network Nation: Human Communication via Computer*, Reading: Addison-Wesley.

Institute for Defense Analysis (IDA) (1997) *National Strategies and Structures for Infrastructure Protection. Report to the President's Commission on Critical Infrastructure Protection*, Washington, DC: IDA. Online. Available at: permanent.access.gpo.gov/lps19700/NationalStrategiesStructures.pdf (accessed 16 October 2007).

Jardini, D.R. (2000) 'Out of the blue yonder: the transfer of systems thinking from the Pentagon to the great society, 1961–1965', in Hughes, A.C. and Hughes, T.P. (eds) *Systems, Experts, and Computers: The Systems Approach in Management and Engineering, World War II and After*, Cambridge: MIT Press.

Joint Committee on Defense Production (JCDP) (1977) *Civil Preparedness Review. Part I: Emergency Preparedness and Industrial Mobilization*, Washington, DC: US Government Printing Office.

Kupperman, R.H. and Smith, H.A. (1972) 'Strategies of mutual deterrence', *Science*, 176, 4030: 18–23.

Kupperman, R.H., van Opstal, D. and Williamson, D. (1982) 'Terror, the strategic tool: response and control', *Annals of the American Academy of Political and Social Science*, 463: 24–38.

Kupperman, R.H., Wilcox, R.H. and Smith, H.A. (1975) 'Crisis management: some opportunities', *Science*, 187: 229.

Lambert, B.K. and Minor, J.E. (1973) *Vulnerability of Regional Electric Power Systems to Nuclear Weapons Effect*, Washington, DC: Defense Electric Power Administration.

Lee, C.P. (2001) *An Exercise in Utility: Civil Defense from Hiroshima to the Cuban Missile Crisis*, doctoral thesis, St. Louis: St. Louis University.

Light, J.S. (2002) 'Urban security from warfare to welfare', *International Journal of Urban and Regional Research*, 26, 3: 607–13.

Light, J.S. (2003) *From Warfare to Welfare: Defense Intellectuals and Urban Problems in Cold War America*, Baltimore: The Johns Hopkins University Press.

Lincoln, G.A. (1973) 'Energy conservation', *Science*, 180, 4082: 155–62.

McMullen, J.K. (2001) *The United States Strategic Bombing Survey And Air Force Doctrine*, Maxwell Air Force Base: School Of Advanced Airpower Studies.

Meilinger, P.S. (1997) 'Giulio Douhet and the origins of airpower theory', in Meilinger, P.S. (ed.) *The Paths of Heaven: The Evolution of Airpower Theory*, Maxwell Air Force Base: Air University Press.

National Security Resources Board (1950) *United States Civil Defense*, Washington, DC: US Government Printing Office.

President's Commission on Critical Infrastructure Protection (PCCIP) (1997) *Critical Foundations: Protecting America's Infrastructures*, Washington, DC: US Government Printing Office.

Quarantelli, E.L. (2000) *Disaster Planning, Emergency Management and Civil Protection: The Historical Development of Organized Efforts to Plan for and Respond to Disasters*, Preliminary paper 301, Newark: Disaster Research Center, University of Delaware.

Roberts, P.S. (2006) 'FEMA and the prospects for reputation-based autonomy', *Studies in American Political Development*, 20, Spring: 57–87.

Stephens, M.M. (1970) *Minimizing Damage to Refineries from Nuclear Attack, Natural, and Other Disasters. A Handbook Reviewing Potential Hazards that Could Affect Petroleum Refinery Operations in Times of War and Peace*, Washington, DC: Office of Oil and Gas Department of the Interior.

Stephens, M.M. (1979) 'Industries: a potential target of terrorists', in Kupperman, R.H. and Trent, D.M. (eds) *Terrorism: Threat, Reality, Response*, Stanford: Hoover Institution Press Stanford University.

United States Department of Defense, Los Alamos Scientific Laboratory (1950) *The Effects of Atomic Weapons*, Washington, DC: US Government Printing Office.

United States Federal Civil Defense Administration (1953) *Civil Defense Urban Analysis*, Washington, DC: US Government Printing Office.

Woolsey, R.J., Wilcox, R.H. and Garrity, P.J. (1984) *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks. A Report of the Panel on Crisis Management of the CSIS Science and Technology Committee*, Washington, DC: Center for Strategic and International Studies, Georgetown University.