

Introduction

“Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.”

Executive Order 13010
President William J. Clinton
July 15, 1996

A quick Google search in 2005 using the term critical infrastructure turns up 650,000 hits, including a wealth of articles and documents. Dig a little deeper into proprietary databases, library catalogs, think tank reports and books, and even more material surfaces.

What’s the fuss about? What is critical infrastructure? Pose the question to the average American and the response is likely to be a blank stare or bemused shrug. But mention water supplies, the electrical grid, banking networks, air traffic control or oil pipelines—and understanding dawns.

The term critical infrastructure—or CI—is relatively new, and its definition elusive and evolving. On the other hand, threats to services and systems that are important to human activity have always been with us, long before *critical infrastructure* became a term of art in policymaking circles.

One of the most obvious—and longest-running—threats to critical infrastructure is Mother Nature, who delivers her message in the form of fires, floods, hurricanes, fallen trees, curious squirrels, earthquakes, lightning and other forces. Anyone whose flight out has been cancelled due to

bad weather, or who has driven miles out of the way to avoid a washed-out bridge, knows that nature has its ways of reminding us of who's boss.

Simple wear-and-tear also poses a constant challenge to critical infrastructure. In the 1980s, a great deal of federal-level attention was devoted to discussing the deteriorating state of the nation's physical infrastructure—the roads, bridges, dams, airports, and similar systems upon which the country depends. The problem is not a small one: nearly four million miles of roadway alone crisscross the country. In its 1988 final report, *Fragile Foundations: A Report on America's Public Works*, a national council gave the nation's infrastructure a C-, "hardly something the world's largest industrial power can be proud of."ⁱ Upkeep, much less expansion, presents an enormous and ongoing infrastructure chore.

Other problems that can plague critical infrastructure include technological obsolescence, poor maintenance, accidents, or that perennial peril: human error. "There are more communications systems taken down per day by the backhoe than by anybody else," notes one infrastructure expert with a touch of humor.

Last, but far from least, intentional destruction of critical infrastructure has always been an issue, albeit a fairly low-key concern during peacetime, until September 11, 2001, when it jumped to the top of the list of federal priorities. It is this last category of potential disruption that has prompted the most recent flurry of federal-level discussion and policy-making related to the nation's infrastructure (and hence, this book).

The strategy of targeting an adversary's vital systems or services for destruction by sabotage or outright attack is far from novel. History offers abundant examples of stratagems designed either to protect one's own critical infrastructure from peril or to destroy that belonging to an adversary, especially during times of war.

To offer but two examples, in ancient Greece, one of Sparta's head warriors, Lysander, seized the Hellespont, the main source of grain imports for Athens, a strategy calculated to starve the city into submission. A weakened Athens tried to fight back but was decisively defeated at Aegospotami. In 1943, the "Casablanca directive" laid out an Allied strategic bombing campaign designed to bring about "the progressive destruction of the German military and industrial and economic system, and the undermining of the morale of the German people to a point where their capacity for armed resistance is fatally weakened."ⁱⁱ Allied bombing

attacks on Germany's railway system after D-Day in 1944 destroyed approximately two-thirds of German rolling stock, slowing delivery of finished goods to the point that the nation's economy was pushed towards collapse.

The main goal, of course, is to destroy—or at least cripple—an adversary's ability to fight, to resupply itself, to communicate, and to function normally. The anthrax scare that shut down a U.S. Senate Office Building in late 2001, for example, appears to have been an attempt to hobble critical infrastructure—in this case, the operations of government.

Destruction isn't always limited to the "enemy's" critical infrastructure. The history of warfare offers many examples of intentional destruction of components of one's own infrastructure—blowing up bridges, for example, to short-circuit the advance of the enemy. Of course, military history also touts the exploits of outfits specially trained to repair or replace such destroyed structures on demand. The U.S. Army's Corps of Engineers excels at throwing bridges across rivers virtually overnight. Their successes at building infrastructure on demand in World War II led General Douglas MacArthur to dub the conflict "an engineer's war."

Naturally, there's a flipside to all of these potential dangers and destructive forces: It's the **defense** of critical infrastructure, or what is today called **critical infrastructure protection or CIP**.

Critical infrastructure protection includes wide-ranging efforts to fortify, insulate and, if need be, quickly repair, rebuild or replace vital systems and services. A few conventional examples include security checkpoints, system redundancies, regularly scheduled back-ups, and preventive maintenance. Even the "Miss Utility" program of areas like Washington, D.C. is an exercise in CIP: the program is designed to keep homeowners from hitting gas, electrical and water lines when excavating for the family swimming pool.

Beginning in the 1980s, the growing use of computers in business and government—combined with the easy accessibility of the burgeoning Internet—added a fresh dimension (and increased urgency) to CIP. Quietly but quickly, much of the nation's most basic infrastructure (e.g. utilities, transportation, banking) came to depend on computers to control many basic functions. Suddenly, not only was the physical infrastructure itself vulnerable to conventional methods of destruction such as explosives, but the overlay of high-tech networks that controlled them was

also a potential target of would-be terrorists, criminals, disaffected employees . . . and bored teenagers equipped with a laptop and ample leisure-time.

Says Phil Lacombe, who worked with the President's Commission on Critical Infrastructure Protection: "We didn't realize that as you pursue the tremendous economic benefits of information systems, you are creating vulnerabilities and dependencies that carried their own seeds of destruction.

. . . It was a revelation for some of the commissioners, as well as for others, that our water systems rely on computer networks and telephone—the ability to use a telephone to dial in to perform maintenance on the water supply system. I didn't think about that stuff before."

Lacombe was far from alone. Most people—except those on the "front lines"—would have had little reason to think about, much less worry about, the perils of increasing interconnectedness. Or to be concerned about how such interconnectedness might prove to be an **Achilles heel in the nation's otherwise formidable defenses.**

"[B]ecause of our cyber dependence, [groups] now had a way of attacking the nation without ever encountering the nation's defense forces," notes Lacombe. "You couldn't fly a bomber at the United States without encountering a radar warning system. You couldn't fire a missile at the United States, anywhere in the world, without encountering a space-based detection capability. You could, however, launch what we called a logic bomb. There are all kinds of names for them, but you could launch an attack, a cyber attack, without ever encountering anything except the public switch network, the Internet, and the World Wide Web."

"We no longer mobilize for war the way we used to," points out Lee Zeichner, a security consultant. "Everything depends on critical infrastructure—soldiers fly out on United Airlines and we use Federal Express. It's so intertwined in how we live that it's a national defense issue."

ENTER PUBLIC POLICY-MAKING.

Because the principal goal of this book is to shed light on the evolution of *federal-level* CIP policy-making, it's useful to place the critical infrastructure protection story within the larger story of how the federal government has responded (or not responded) to (perceived or real) threats to critical infrastructure over the past two centuries and more.

Doing so requires looking at the overall picture of the nation's attitude and actions to protect itself, especially on its home turf, in response to changes in adversaries, weaponry, citizen demands and domestic politics. A common umbrella term for this effort is *preparedness*.

Not surprisingly, the most visible and vociferous public debates about the nation's level of preparedness have come during times of major disasters or heightened fears of attack. Examples include: during World Wars I and II, after the U.S.S.R. successfully detonated an atomic bomb in 1949 and a hydrogen bomb in 1953, following the Cuban Missile Crisis of 1962, and after the events of September 11, 2001.

Among the "big" questions that have driven the national preparedness debate since the beginning are such sticky issues as how much preparedness is enough? How much is too much? What's worth protecting? At what cost? Whose responsibility is it, anyway? Federal? State? Local? Private? And who's going to ante up?

Today, post-September 11, the debate over the appropriate level of general preparedness (now called homeland defense or homeland security) is once again raising controversial questions about the quality and quantity of laws, regulations and resources that should be devoted to 'securing security.' As well as the costs and responsibilities/roles of various parties. Naturally, the nation's critical infrastructure and its protection are part of this larger debate.

This slim volume doesn't pretend to paint a full-blown and detailed picture of American preparedness policy since the nation's founding. Scholars have devoted thousands of pages to examining such policy-making in minute detail. Instead, we offer a primer, one that will paint the proverbial "big picture" of preparedness policy, while encouraging inquisitive readers to delve into specifics via the bibliography and materials that can be found on our CIP Oral History website: URL: <http://echo.gmu.edu/cipp>.

In these pages, we highlight key events and developments in the evolution of official thinking on such (often overlapping) preparedness issues as civil defense, industrial mobilization, and emergency management—up to and including the work of the President's Commission on Critical Infrastructure Protection (1996–1997), where our story ends.

In the process, we'll touch on factors that have informed the CIP debate over time. For example:

- Changes in what is considered critical infrastructure. How our perception of “critical” has changed or remained the same over the past three centuries.
- The (often inherently) conflicting agendas of public and private sector interests in the level and types of security devoted to critical infrastructure.
- The fact that the majority of the nation’s CI is in private—not governmental—hands, which raises the sticky question of proper roles and responsibilities of federal, state, local government and the private sector in CIP.
- Modes of making and delivering threats. How evolving technologies have altered the ways in which nation states, groups or individuals can threaten populations, undermine public confidence, disrupt or compromise critical systems.

And, finally, the human response to threats: How fear and complacency have influenced public willingness over time to support or question governmental initiatives to institute policies in the name of “national security.”

ⁱ National Council on Public Works Improvement, *Fragile foundations: a report on America’s public works: final report to the President and the Congress* (Washington: GPO, 1988): 2.

ⁱⁱ Gerhard L. Weinberg, *A World at Arms. A Global History of World War II* (Cambridge: Cambridge University Press, 1994).