

COPYRIGHT NOTICE:

**Charles Perrow: The Next Catastrophe**

is published by Princeton University Press and copyrighted, © 2007, by Princeton University Press. All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher, except for reading and browsing via the World Wide Web. Users are not permitted to mount this file on any network servers.

Follow links for Class Use and other Permissions. For more information send email to: [permissions@pupress.princeton.edu](mailto:permissions@pupress.princeton.edu)

# 1 Shrink the Targets

---

DISASTERS FROM NATURAL sources, from industrial and technological sources, and from deliberate sources such as terrorism have all increased in the United States in recent decades, and no diminution is in sight.<sup>1</sup> Weather disturbances are predicted to increase; low-level industrial accidents continue but threaten to intensify and the threat of cyber attacks on our “critical infrastructure” becomes ever more credible; foreign terrorists have not relaxed and we anxiously await another attack. Cataclysmic fantasies proliferate on movie screens and DVDs, and scholars write books with “collapse,” “catastrophe,” “our final hour,” and “worst cases” in their titles.

But we have neglected a fundamental response to the trio of disaster sources. Instead of focusing only on preventing disasters and coping with their aftermath—which we must continue to do—we should *reduce the size of vulnerable targets*. Weapons of mass de-

<sup>1</sup>The evidence for the increase in industrial disasters comes from the Swiss reinsurance firm, the world’s largest, Swiss Re. The worldwide figures can be found in its Sigma reports. (Swiss Re 2002) “Man-made disasters” include road and shipping accidents, major fires, and aerospace incidents, and the threshold for qualifying is 20 deaths, or 50 injured, or 2,000 homeless, or \$70 billion in losses, or insurances losses ranging from \$143 million for shipping, \$28 billion for aerospace to \$35 billion for the rest. Similar criteria are applied to natural disasters. For man-made disasters in the United States, the period from 1970 to 1992 averaged 7.7;

struction (WMDs) already litter our landscape; terrorists need not sneak them in, and they are more likely to be triggered by natural and industrial disasters than by terrorists. Ninety-ton tank cars of chlorine gas are WMDs that travel daily through our cities; dispersing the deadly gas via a tornado or hurricane, an industrial accident, or a terrorist's suitcase bomb would endanger up to seven million people. New Orleans and its surroundings is, or was, our largest port, but it could have been a target one-third the size of its pre-Katrina population of some 450,000 souls, and much easier to defend and evacuate. Because of the increased concentration of the electric power industry, our vital electric power grid is so poorly managed that sagging power lines hitting tree branches in Ohio plunged the Northeast into darkness for hours and even days in some areas in 2003. The industry has made its grid a better target for a heat spell, a flood, a hurricane, or a few well-placed small bombs. Deconcentrating the industry would uncouple the vulnerabilities and barely decrease efficiency, as we shall see.

Not all of the dangers confronting us can be reduced through downsizing our targets. Some natural hazards we just have to face: we are unlikely to stop settling in earthquake zones, nor can we avoid tsunamis, volcanoes, asteroids, or even tornadoes. Even small targets are at risk in the case of epidemics, and terrorists with biological and radiological weapons can cause such widespread devastation that the size of the target is irrelevant.

But, except for tornadoes, all these are rare. Devastations from the more common sources such as high winds, water and fire dam-

---

from 1993 to 2001 it was 12.8, a 60 percent rise. (Special tabulation provided by Swiss Re.) Natural disasters rose steadily in this period, well below the man-made ones in the 1970s but rising to almost thirty a year for the period 1993 to 2001. Data on terrorist attacks and casualties are harder to come by, but following the end of Algerian, Italian, and Irish terrorist activity in the 1970s and early 1980s, there was a decline. But there has been a rise in the 1990s to the present. The number of "significant" international terrorists attacks has increased eightfold in the last over the last two decades, according to an analysis of U.S. government data presented in the *Human Security Report*. There has also been a clear but uneven upward trend in the number of casualties from international terror, between 1982 and 2003. (Centre 2005, 32)

age, industrial and technological accidents, and terrorist attacks on large targets can be greatly reduced. It will not be easy, but given our yearly disaster bill in the billions of dollars, it makes economic sense as well as social sense. It will require a change in our mindset about markets and regulation. Since our current mindset is only decades old—it changed quickly from the 1970s on—it is hardly inconceivable that it could not change again.

Disasters expose our social structure and culture more sharply than other important events. (Clarke 2005) They reveal starkly the failure of organizations, regulations, and the political system. But we regard disasters as exceptional events, and after a disaster we shore up our defenses and try to improve our responses while leaving the target in place. However, as Clarke persuasively argues, disasters are not exceptional but a normal part of our existence. To reduce their damage will require probing our social structure and culture to see how these promote our vulnerabilities. We will do this throughout this book in the hope of prodding changes in these areas.

Two of the major themes in this work are the inevitable failure of organizations, public and private, to protect us from disasters and the increasing concentration of targets that make the disasters more consequential. There are many explanations for the first theme, organizational failures, but we will highlight one in particular: organizations are tools that can be used for ends other than their official ones. To prevent unwarranted use, we require regulation in the private sector and representative governance in the public sectors. The failure of the political system means ineffective regulation. This can be changed.

One goal of regulation is to prevent the accumulation of economic power in private hands. Otherwise, we get the concentration not just of economic power but of hazardous materials, populations in risky areas with inadequate protection, and vulnerabilities in parts of our critical infrastructure such as the Internet, electric power, transportation, and agriculture. (We also need regulation to ensure that the public sector is not wasteful, that standards are adequate to protect us, that corruption is minimized, and so on.) The

third major theme concerns a structural alternative to the concentrations that endanger us. We encounter it first in the electric power grid and second in the Internet; these are networked systems, rather than hierarchical systems. Networks are decentralized, with minimal concentrations of destructive energy and economic power. They are efficient, reliable, and adaptive, which minimizes the dangers of organizational failures. In the grid and the Internet, they are being challenged by consolidating forces, but these can be resisted. We explore the advantages of networks in the final chapter, where we examine networks of small firms, and terrorist networks.

### THE CONVENTIONAL VIEW

In contrast to the approach taken here, which is to reduce concentrations of the things that make us most vulnerable, most efforts either accept such concentrations as inevitable or don't notice them at all and focus on responding to disasters, limiting the damages, and preventing disasters. All three strategies are necessary and should be vigorously pursued, but their limitations are apparent.

*Responding* to disasters involves “first responders,” such as police, fire, and voluntary agencies. (Lee Clarke calls them “official first responders,” since the friends, family, or coworkers of victims and also passerbys are always the first and most effective responders.) We have not done well here. We are barely equipped for the routine fire, flood, or explosion and fail dramatically with the big and unexpected disasters. Our new Department of Homeland Security is often criticized by the Government Accountability Office (GAO) and public policy organizations for its woefully inadequate first-responder funding. The title of a 2003 Council on Foreign Relations task force report summed up the problems: “Emergency Responders: Drastically Underfunded, Dangerously Unprepared.” (Rudman, Clarke and Metzl 2003) This was apparent in the 2005 Katrina hurricane.

Furthermore, we have a “panic” model of behavior, which mistakenly limits information, which in turn breeds skepticism on the

part of the public. Years of research on disasters indicates that panic is rare, as is rioting and looting, and that the very first responders are citizens whose capacity for innovative response is impressive. The panic model unfortunately legitimates the tendency to centralize responses thus both curtailing citizen responses and interfering with the responses of the lowest-level agencies, such as police, fire, medical teams, and voluntary agencies. Research shows the most effective response comes when such decentralized units are free to act on the basis of firsthand information and familiarity with the setting. (Clarke 2002; Quarantelli 1954; Quarantelli 2001; Tierney 2003) The panic model can even make things worse. Disaster expert Kathleen Tierney shows how the media's penchant for the panic model probably caused unnecessary deaths in the Katrina disaster. (Tierney, Bevc, and Kuligowski 2006)

*Limiting damage* involves building codes, which cover structural standards and require protection of hazardous materials, and evacuation plans. There have been improvements here, but it is unlikely they will ever be enough. Government organizations often do not enforce codes; evacuation plans are unrealistic or unimplemented (as Katrina showed); inventories of hazardous materials (commonly called *hazmats*) are not made; local interests defy national standards on building sites (if these even exist); and our Supreme Court has eviscerated floodplain and wetlands regulations that would limit flood damages.

Finally, *preventing* disasters that involve vulnerable targets is the most developed of the three strategies, perhaps because there are more profits for private industry to be found in expensive prevention devices than in training and funding first responders or in following building codes. Here we have alarms and warning systems for natural and industrial dangers; and for terrorism we have biochemical sniffers and suits, border and airport inspections, covert surveillance of citizens, and encryption for our electronic transmissions and interception of those of other nations. The economic opportunities here are substantial, so substantial that one angry review of the Department of Homeland Security (DHS) after the Katrina disasters spoke not of mismanagement, or even graft, but of

outright “looting” of the public treasury (Klinenberg and Frank 2005). A front-page article in the *New York Times* about Katrina and the DHS was titled “‘Breathtaking’ Waste and Fraud in Hurricane Aid.” (Lipton 2006b) One lawyer for a prominent Washington DC law firm was up front about corporate interests: he wrote a newsletter article titled “Opportunity and Risk: Securing Your Piece of the Homeland Security Pie.” (Shenon 2003a; Shenon 2003b) It is a very large pie indeed.

The Department of Homeland Security is virtually a textbook example of organizational failure that impacts all three of our disaster sources. For example, the Federal Emergency Management Agency (FEMA), once a model organization, was moved into the DHS, its budget for natural-disaster management was cut, its authority to coordinate emergency responses was taken from it, and it was staffed with inexperienced political appointees. (Staff 2005c) It became an extreme case of “permanently failing organizations” (Meyer and Zucker 1989)—those that we cannot do without but, in addition to the human fallibility of their members, are beset by underfunding in the public sphere, used for ends they are not designed for, and shackled with bad rules and regulations.

## OUR VULNERABILITIES

There is little consideration by policy makers of the possibility of reducing our vulnerabilities, rather than just prevention, remediation, and damage limitation. (Steven Flynn’s book, *America the Vulnerable* [2004] is one of the few attempts to explore this. Allenby and Fink [2005] imply target reduction in their discussion of resiliency in societies.) Yet, it would be the most effective in the long run.

The sources of our vulnerabilities are threefold:

- The first are *concentrations of energy*, such as explosive and toxic substances (largely at industrial storage and process industries), highly flammable substances (e.g., dry or diseased woods, brush), and dams (one of the concentrations we can do little about).

- The second are *concentrations of populations* (in risky, even if desirable, areas), and especially when high-density populations also contain unnecessarily high concentrations of explosive and toxic substances, such as ruptured oil storage tanks in the case of Katrina and propane tank farms in St. Louis that were nearly set off by a huge flood.
- The third are *concentrations of economic and political power*, as with concentrations in the electric power industry, in the Internet (e.g., the “monoculture” Microsoft has created with the Windows operating system), and in food production such as beef and milk.

The three sources are interrelated. Concentrations of economic and political power allow the concentrations of energy, generally by means of deregulation, and these tend to be where there are concentrations of populations. To give a minor example, deregulation of the airlines started with President Carter and led initially to more airlines, more competition, and lower fares—all favorable results. But starting in the 1990s, the number of airlines decreased as the industry reconcentrated because of weakened antitrust concerns in the government. The airlines concentrated their routes through the hub-and-spoke system, which encouraged the use of ever larger aircraft as smaller flights were channeled into one hub, and passengers were then flown en masse to key destinations. Because of the concentrated hub-and-spoke system, simple industrial accidents, computer breakdowns, or false alarms at major airports now can paralyze whole sections of the nation. The attempted terrorist attack on the Los Angeles airport in December 1999 would have disrupted far more traffic than one under the regulated system. And when nature, software failures, or terrorists bring down the new airplanes carrying 550 passengers, we will realize our vulnerability to the inevitable failures of airplanes, pilots, and controllers has increased just a bit.

But the concentrated airline industry is only a relatively small instance of the increased size of our targets; we will examine larger ones in the following chapters, starting with the first of our trio of mounting threats, natural forces. The forces have not increased

much (*how* much is in dispute), but our vulnerable concentrations have greatly swollen. I will argue in the final chapter that our emphasis on the terrorist threat is exaggerated. It is a threat, but not as certain or consequential as those of natural forces and industrial and technological accidents. Were the terrorist threat to disappear, I would still recommend all the deconcentrations presented in this volume.

## THE ARGUMENT

I will start with the easiest argument in chapter 2: natural disasters, with emphasis on floods and hurricanes. Thanks to their increasing prosperity in the past half-century and a fortunate lull in patterns of extreme weather, people have moved closer to the waterfront. Their concentrated settlements are imperfectly regulated and thus are vulnerable to storms while lacking evacuation provisions. Perverse incentives in the form of subsidized insurance and federal reconstruction funds, combined with powerful local growth policies, increase our losses from natural disasters every decade. We will consider the Gulf Coast, a Mississippi River flood, and the numerous vulnerabilities of California.

Part 2 concerns the formal governmental response to disasters. Initially these were mainly natural disasters, and chapter 3 examines the government's response to disasters past. Surprisingly, the substantial role the federal government plays in helping with disasters is only about sixty years old, and I will examine that short history and in particular the role of FEMA, the key disaster agency. We will see that for a time it was an effective agency, one of the few effective ones that we will examine, but that twice in its history it has been hijacked for other purposes by presidents Ronald Reagan and George W. Bush. A model agency in the mid-1990s, it was made dysfunctional in 2001. We shall see why in chapters 3 and 4.

Disasters have other causes besides nature, and chapter 4 considers our response to terrorist threats (and the implications for FEMA). While the nation has always had domestic terrorist threats,

the scope of the 9/11 attacks prodded the federal government to do something more concerted than leaving the threat of foreign terrorist to be handled by intelligence agencies, border patrols, the FBI, and local police. This attempt by our government gives us the short and sorry history of the Department of Homeland Security, the largest federal reorganization ever. Its history illustrates well the difficulty of creating effective organizations.

We should not expect too much of organizations, but the DHS is extreme in its dysfunctions. As with all organizations, the DHS has been used by its masters and outsiders for purposes that are beyond its mandate, and the usage of the DHS has been inordinate. One major user of the DHS is Congress. While Congress is the arm of the government that is closest to the people, it is also the one that is most influenced by corporations and local interest groups that do not have the interests of the larger community in mind. Chapter 4, on the DHS and the intelligence reorganization, is mainly focused on the government, but our vulnerabilities are increasing in the private sector, and that is what we turn to in the four chapters of part 3.

Much of our critical infrastructure is in the hands of large corporations and, like our government, these private organizations are prone to error, in the form of industrial accidents as well as their failure to provide ample protection from natural and terrorist disasters. These risks are national in scope, rather than confined to an area impacted by hurricanes or floods. The private sector contains some of the largest vulnerable concentrations with catastrophic potential.

We will start with the nuclear power industry, in chapter 5, which carries the fearsome potential of a nuclear meltdown that could, as one famous report said just before the Three Mile Island near miss, irradiate an area half the size of Pennsylvania. Organizational and regulatory failures abound in this poorly regulated enterprise. Beyond the inevitable but prosaic failures of organizations, however, we will encounter here very good evidence of what will be called “executive failure,” where the chief executive ignores the warnings of his staff and forces them to conduct unsafe prac-

tices. Given the size of the potential disaster in this case, such executive failures are frightening. There is a sinister side to organizational failures—not all are just prosaic—and where national safety is concerned, we should be especially concerned. As Diane Vaughan, the chronicler of space-shuttle failures, points out, this “dark side” of organizations is missing from the conventional literature. (Vaughan 1999) We shall also see how the regulatory agency bows to industry pressure and cuts back on inspections. And, of course, there is the inept attempt to deal with the terrorist threat.

Next we will examine the chemical industry in chapter 6, a vital industry that has provided better living through chemistry even while we suffer from its mostly hidden depredations. Despite its claims, it has done little to reduce the threat of terrorism, and its targets are perhaps the most poorly defended and the easiest to attack with garden-variety weapons. The danger is not just in the lack of protection from terrorists but in the huge concentrations of explosive and toxic materials, since these are also vulnerable to natural disasters, as in the case of oil spills because of Katrina. The concentrations are also vulnerable to industrial accidents, where the steady death toll could rise substantially as concentration of hazardous materials increases, along with the pressures to increase the use of unqualified contract workers in risky “turnaround” operations.

The chemical industry’s record on self-regulation is not good. By claiming that they meet their trade association standards of low pollution, chemical companies escape federal inspection and pollute more. Bigger is not safer in this industry; the larger companies and the larger plants pollute more and have more accidents. Congress has been unable to set higher standards; useful bills are locked up in Republican-controlled committees. The Supreme Court declared that New Jersey’s higher standards are invalid; the lower federal standards will prevail. Pressure from public interest groups has made the industry more responsive to some product safety and pollution concerns, so there is encouragement here, but these groups are not pursuing the more consequential issues of safer processes and smaller hazmat inventories.

The third conventional industry, and the single most vital one in our critical infrastructure—electrical utilities—is considered in chapter 7. The individual plants that produce electricity are vulnerable to our three sources of disaster but only moderately so. We will be much more concerned with the electric power grid. Concentration in the industry, as a result of deregulation that speeded up in the late 1990s, has resulted in business plans by the utilities that minimize investment in transmission but instead perversely overload the burdened, unmodernized grid with long-distance transmissions that reap small benefits in cost in return for large risks of cascading failures and a large increase in vulnerability to deliberate attacks, accidents, and weather. Industry self-regulation again encourages cheating on safety and reliability.

Another aspect of the grid that we will examine closely is the effects of deregulation. Before extensive deregulation, which did not lower the price of electricity but increased industry profits, the grid was remarkably efficient and reliable, self-adjusting to a limited degree, and able to handle increases in transmission without increases in blackouts. This illustrates the potential for network forms of organization rather than our traditional hierarchical forms, which will also be explored in chapters 8 and 9. These forms offer more reliability and resiliency, and less vulnerability, and could be models for other aspects of our critical infrastructure.

The public is aware of the scale and degree of the natural disaster hazard and the failures of FEMA and even the DHS, but it is largely unaware of the hazardousness of the chemical, nuclear, and electric power industries. It is even less aware of the hazard potential of the Internet, examined in chapter 8, our final industry chapter. As with the power grid, there is a resilient aspect to the Internet and World Wide Web but also a vulnerability that could make accidents or deliberate attacks very consequential. The vulnerability lies largely in the monopoly power of the Microsoft Windows operating system and the threatened consolidation of internet service providers (ISPs). Even more than the power grid, the Internet is a remarkable, vast, decentralized, resilient system that could be a model for some of our other critical industries. The threats to it

come from lack of regulation as a common carrier—we will examine this “open access” or “net neutrality” issue—and the profit potentials that come with concentration. These open the Net to easier attack, not just from viruses and hackers but from terrorists. Terrorists could disable power plants, including nuclear ones, tamper with the files of intelligence agencies, read the plans of the Department of Defense, and assault the banking sector. Hackers already have done these things.

Part 4 contains the final chapter. It brings together several of the themes and explores the costs and opportunities of deconcentrating our most vulnerable targets. One crucial question is whether the attempt to reduce the size of targets entails a loss of efficiency that is presumably gained with the economies of scale that come with large corporations. An obvious answer is that, given the disaster potential, we should be prepared to pay a bit more to reduce our vulnerability. The costs of Katrina, the 2003 northeastern power blackout, the Baltimore railroad tunnel fire, and many other such disasters greatly outweighed the expenditures that could have prevented them. A more subtle answer is to distinguish dependencies from interdependencies in our highly interconnected world. Many dependencies can and should be avoided, and instead we should reorganize to maximize the values of interdependency. In some notable cases, this increases economic efficiency as well as reducing vulnerabilities.

Chapter 9 will also revisit the terrorist threat. In the industrial chapters I have placed it more or less on a par with threats from nature and from industrial accidents. But in chapter 9 I will explore the idea that we have spent too much on the very remote possibility of another massive terrorist attack, and with little benefit given our basic vulnerabilities; and far too little on natural and industrial disasters, which are certainties; and next to nothing on target reduction. I examine the reasons why we are much more likely to experience small-scale foreign terrorist attacks than the massive ones involving weapons of mass destruction we spend most on preventing, and I argue that neither of these can receive anything like adequate protection. What will matter most is deconcentrating vulnerable targets.

Finally there is the question of whether it is even possible to deconcentrate populations, hazardous materials, and powerful organizations such as Microsoft and the electric power industry. Throughout the book I will suggest, in connection with each risky system, that this is quite possible, and I bring the arguments together at the end. Political changes over the last three or four decades have made it more difficult, but these are reversible.<sup>2</sup>

<sup>2</sup>We will not explore the ways in which the poor and minorities bear most of the brunt of disasters. They are indeed the population most “targeted” in natural and industrial disasters. The classic work on this is Bullard 1990. See also Mohai and Bryant 1992; Schnaiberg 1983; and for prescient work dealing with oil and chemical plants near New Orleans see Allen 2003. A classic broader view is Erikson 1994. For a quite different view, see “Richer is sicker versus richer is safer,” a chapter in Wildavsky 1988, 59–75.