CHAPTER 32

Disasters Ever More? Reducing U.S. Vulnerabilities[1]

Charles Perrow

Natural disasters, unintended disasters (largely industrial and technological), and deliberate disasters have all increased in number and intensity in the United States in the last quarter century[2] (see Figure 32.1) In the United States we may prevent some and mitigate some, but we can't escape them. At present, we focus on protecting the targets and mitigating the consequences, and we should do our best at that. But our organizations are simply not up to the challenge from the increasing number of disasters. What we can more profitably do is reduce the size of the targets, that is, reduce the concentrations of energy found in hazardous materials, the concentration of power in vital organizations, and the concentrations of humans in risky locations. Smaller, dispersed targets of nature's wrath, industrial accidents, or terrorist's aim will kill fewer and cause less economic and social disruption.

Not all of the dangers confronting us can be reduced through downsizing our targets. Some natural hazards we just have to face: we are not likely to stop settling on earthquake faults nor can we avoid tsunamis, volcanoes, and tornadoes. Epidemics and terrorists with biological and radiological weapons can cause such widespread devastation that even small targets are at risk. But all these are rare. The more common sources of devastation, such as wind, water, and fire damage; industrial and technological accidents; and terrorist attacks on large targets, can be greatly reduced.

Why are we doing so poorly? Because the targets are becoming larger, and because our organizations—relief organizations, Congress, and government at all levels—will never

[1] I am grateful for support from a National Science Foundation Small Grant award, SES-0329546.

[2] The evidence for the increase in industrial disasters comes from the Swiss reinsurance firm, the world's largest, Swiss Re. The world-wide figures can be found in their Sigma reports (Re, 2001). 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 2000 homeless, or $70 billion in losses, or insurance 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; from 1993 to 2001 it was 12.8, a 60% 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 30 a year for the period 1993 to 2001. Data on terrorist attacks and casualties is 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.

NATURAL: Increased interdependencies of natural and constructed environments.

Meteorites Volcanoes Hurricanes Floods Droughts
Earthquakes Tsunamis Forest fires Epidemics

UNINTENDED: Increased scale and lethal potential of industry and technology.

Fires, explosions Transportation accidents Toxic Wastes
Toxic releases Genetically engineered crops Software

DELIBERATE: Increased unrest, vulnerability, lethal weapons

Cyber attacks (beginning) Sabotage (minor) Dementia (rare)
Terrorism (mounting: more lethal weapons, consequential targets,
radical religious sects, and more international inequality and
political disorder)

Figure 32.1. Types of disasters.

be up to the task of reasonably protecting us. I will first go through some of the familiar problems with the agencies responsible for prevention, mitigation, and remediation; then turn to some deconcentration possibilities; and finally, outline the general principles that will allow us to build economical, reliable, decentralized networks in our critical infrastructure, with four examples of such systems.

ORGANIZATIONS: PERMANENTLY FAILING

Remediation, or responding to damage, involves "first responders," such as police and fire and voluntary agencies. We have not done well here. For one thing, a repeated criticism of our new Department of Homeland Security (DHS) by the Government Accountability Office (GAO) and public policy organizations is that first responder funds are woefully inadequate. The title of a 2003 Council of Foreign Relations taskforce report summed up the problems: "Emergency Responders: Drastically Underfunded, Dangerously Unprepared" (Rudman, Clarke, & Metzl, 2003). This was apparent in the 2005 Katrina hurricane. Further, 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 indicate that panic is rare, as is rioting and looting, and the "very first" responders are citizens whose capacity for innovative response is impressive. The panic model unfortunately legitimizes 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 first-hand information and familiarity with the setting (Clarke, 2002; Tierney, 2003).

Limiting damage involves building codes that 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. Organizations do not enforce codes, evacuation plans are unrealistic or not implemented (as Katrina showed), and inventories of hazmats are not made.

Finally, preventing damage is the most developed, 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 snifters and suits, border and airport detection, and encryption for electronic transmissions. The economic opportunities here are substantial. As soon as the DHS was established, the corporate lobbying began. Four of Secretary Tom Ridge's senior deputies in his initial position as Assistant for Homeland Security at the White House left for the private sector and began work as homeland security lobbyists, as did his legislative affairs director in the White House. The number of lobbyists who registered and listed "homeland," "security," or "terror" on their forms was already sizable at the beginning of 2002, numbering 157, but jumped to 569 as of April, 2003. One lawyer for a prominent Washington, DC law firm was up-front about corporate interests. He mentions in his online resume that he authored a newsletter article titled "Opportunity and Risk: Securing Your Piece of the Homeland Security Pie" (Shenon, 2003a, 2003b). It is a very large pie indeed.

The DHS is virtually a textbook of organizational failures that impact all three of our disaster sources.[3] For example, the Federal Emergency Management Agency (FEMA), once a model organization, was moved into the DHS and its budget for natural disaster management slashed, its authority to coordinate emergency responses taken from it, and its staffing positions filled with political appointees throughout (Hsu, 2005; Isikoff & Hosenball, 2005; Writers, 2005). It became an extreme case of what sociologists call "permanently failing organizations" (Meyer & Zucker, 1989), those that we cannot do without but that we underfund, use for ends they are not designed for, shackle with bad rules and regulations, and so on. It is what we would expect, regardless of the political party in power. We can always try harder, but we should be prepared for inevitable failures.

A MORE PROMISING RESPONSE: REDUCING VULNERABILITIES

There is little consideration by policymakers of the possibility of reducing our vulnerabilities, rather than just prevention, remediation, and damage limitation. (Steven Flynn's 2004 book, *America the Vulnerable,* is one of the few attempts to explore this.) 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 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, though desirable areas), especially when high-density populations also have high concentrations of explosive and toxic substances.
- The third are *concentrations of economic/political power*, as with concentrations in the electric power industry, in the Internet (e.g., the "monoculture" Microsoft has created), and in food production such as beef and milk.

The three are interrelated. Concentrations of economic and political power allow the concentrations of energy, generally by means of deregulation, and these tend to be where

[3] For details, see C. Perrow, "The second disaster: the department of homeland security and the intelligence reorganization," unpublished manuscript, Department of Sociology, Yale University, 2004, available upon request from charles.perrow@yale.edu.

there are concentrations of populations. To give a minor example, the airline industry, and its catastrophic potential, increased with deregulation. Deregulation 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 declined with reconcentration, made possible because of weakened antitrust concerns of government. They concentrated their routes through the hub and spoke system; and this encouraged ever larger aircraft. Because of the concentrated hub and spoke system, simple industrial accidents or computer breakdowns at major airports now 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 an attack under the regulated system. And when nature, software failures, or terrorists bring down the new airplanes with more than 500 passengers aboard we will realize our vulnerability has increased. But the concentrated airline industry is only a minor instance of increasing the size of our targets.

Deconcentrating Chemical Production and Storage

More important is the massive concentrations of hazardous materials in our chemical plants. The industry has seen extensive consolidation since the 1960s and increasing plant size (Lieberman, 1987). The industry averages five accidents a day, and kills from 250 to 260 people a year (Purvis & Bauler, 2004). But this is hardly noticed since it is usually only two or three at time, and they are almost always workers. (Think of the outrage if we had comparable fatalities from two 727 crashes each year, killing businessmen and others who are able to afford air travel.) Economies of scale abound in this business. A doubling of plant capacity increases the capital costs by only about 60%, so bigger is cheaper (Ashford, 1993, III-9). Bigger facilities also mean bigger targets and bigger catastrophes, and the losses have been increasing. Writing in 1993, Ashford et al. say “A survey of the largest property losses over the past 30 years indicates an increase of 500 percent in the average size of the loss, holding prices constant.” They add that a study by the Organization for Economic Cooperation and Development (OECD) notes that, in the post–World War II period, “The incidence of major industrial accidents was only one every five years or so, until 1980. Since 1980, the incidence has risen to two major accidents per year” (Ashford, 1993, III-9). The industry claims that it is safer than manufacturing industries, but the workers most at risk are “contract workers,” hired for short-term jobs from companies that the government classifies in various construction industry categories rather than the chemical industry. Since 30% of the workforce is contract workers, and they are the most likely to have accidents, the claim that the industry has one of the highest safety records is without merit (Perrow, 1999, pp. 361–362).

The potential for catastrophe is immense, and the trigger could be a storm, an industrial accident, or a terrorist attack. Facilities with significant amounts of chemicals had to prepare worst case scenarios for the Environmental Protection Agency (EPA). A remarkable Washington Post story summarizes some of the findings (Grimaldi & Gugliotta, 2001). A single railcar of chlorine, if vaporized near Los Angeles, could poison 4 million people. Four million people could be harmed by the release of 400,000 pounds of hydrogen fluoride that a refinery near Philadelphia keeps on hand. A chlorine railcar release near Detroit would put three million at risk. Union Carbide’s Institute, WV plant near Charleston once again has 200,000 pounds of methyl isocyanate, the chemical that did so much damage in Bhopal, which would threaten 60,000 people. (Union Carbide had removed the methyl isocyanate storage from the Institute plant after the Bhopal accident, but the Institute plant was reported to be storing it again in

2001 [Staff Writers, 2001]). And close by New York City, a plant in New Jersey has 180,000 pounds of chlorine and sulfur dioxide that could create a toxic cloud that would put 12 million people at risk (Grimaldi & Gugliotta, 2001). These scenarios assume that there is no collateral damage to nearby processes or storage facilities in the plant, but that damage could make it worse.[4]

Is it possible to reduce these concentrations? There are some significant examples of both substituting safer processes or substances, and reducing storage inventories, indicating that it is quite possible and not economically damaging (Ashford, 1993, II-18; Purvis & Bauler, 2004, p. 10). But considering the thousands of vulnerable sites, a dozen examples are only a drop taken from the chemical bucket. Nor is bigger safer. Both Howard Kleindorfer and Don Grant have studies showing the larger the plant the more unwanted releases, even controlling for size of inventory Grant & Jones, 2003; Grant, Jones, & Bergesen, 2002; Kleindorfer et al., 2003).

One objective that is certainly possible is to reduce these concentrations in concentrated populations. Regulations here are very weak, and the concentrations have only very small economic justifications. Large amounts of diesel fuel were stored in the deepest basement of the World Trade Center, and the fuel almost ignited when the building was destroyed. Its ignition would have wreaked much greater devastation than we already had. The economic savings of such storage were trivial. Railroad cars containing 60 tons of deadly chlorine gas sit idly on side tracks within blocks of the White House in Washington, DC, vulnerable to a railroad accident, a lightening strike, or a suitcase bomb. They either should not be there or should not go through downtown Washington; alternatively, they could be transported in smaller amounts in more rugged containers.

Would more containers increase the likelihood of more disasters? Smaller containers are easier to protect, and easier for workers to handle; they present less surfaces for storms to attack; and their value to terrorists would be much lower. Assume one storage facility is dispersed over 10 widely spaced locations, say a few miles. Terrorist would have to coordinate 10 attacks to realize the damage of a single concentrated one. A disaster at the concentrated facility is more likely to endanger nearby containers or processes with hazmats, and interfere with the ability to man safety systems and recovery efforts. The drawback is that more transportation, and its accident potential, is involved with dispersion, but the quantities are smaller and protection easier. In the face of all three threats, smaller means safer, and this can justify the increased costs.

Deconcentrating Populations

Deconcentrating populations in risky areas is much more difficult. Katrina has done it temporarily in New Orleans, but given the economic importance of the port, it is likely to be rebuilt. It not only drains our Midwest river system of most of the nation's agricultural products, but is the inlet for Latin American raw materials and the distribution node for a quarter of our oil and gas supplies. Given the absence of tough, enforced, building regulations in a state such as Louisiana, a rebuilt New Orleans is not likely to be significantly safer from a direct hit from a future force 4 or 5 hurricane. (Katrina was a softened blow; had it been a few miles west the inrush of water from the storm surge would have meant only 2 to 3 minutes, instead of several

[4] For details, see C. Perrow, "Better Vulnerability Thru Chemistry," unpublished manuscript, Department of Sociology, Yale University, 2004, available upon request from charles.perrow@yale.edu.

hours, to get up to the attic and break through to the roof. Katrina is a certified "worst case," but as Lee Clarke says, worst cases can always be even worse (Clarke, 2005). We are not going to abandon the San Andreas, California, earthquake fault with its cities, hazmat storage tanks, and it nuclear plant. (A large earthquake would depopulate it thoroughly.) The ports at and around Los Angeles are marvels of concentrated economic efficiency. An earthquake, tidal wave, domino of explosions, or a dirty bomb in a shipping container would halt much of the economic activity of California (and Hawaii) for months (Flynn, 2004).

Little can be done, beyond what nature, industrial accidents, or terrorists would do, to deconcentrate risky areas. But effective regulation would make a dent and reduce the amount that the nation pays to subsidize the losses of those who enjoy the water views and warm climates. The United States tries and fails each time there is a disaster to withhold funds from those who failed to buy insurance, already heavily subsidized. (This goes for Midwest floods of farm lands, where the water views are not the incentive to settlement.) Gradually, we improve building standards and impose zoning requirements that limit our vulnerability, but the real estate interests' goal of growth and our appetite for lovely settings makes it difficult. As the seas rise and move inland, and populations continue to move to the coast, we should look to the system that the Netherlands has imposed. Most of that lovely country is below sea level, and while it does not have hurricanes, it has significant storm surges that have drowned a good part of it in the past. A strong central government builds and maintains dikes, houses in some areas must be built to float, and zoning disperses the population. The erosion that industry and government has allowed to happen in the alluvial Louisiana delta would be unthinkable in Northern Europe. The ocean and the storm surges are moving closer to New Orleans every year, and experts and government officials have been aware of it for at least since the middle of the last century. Our "permanently failing organizations" could be up to the job of reducing vulnerabilities rather than just increasing our protection and recovery attempts. We make a little progress with each disaster. With increased awareness of our vulnerabilities we could make much more.

Deconcentrating Organizations

The case for deconcentrating large organizations that are at the center of our critical infrastructure will be limited to only two illustrations: the Internet, and even more vital to our connected society, the electric power grid. (Cases can be made for deconcentration in the raising of cattle, bulk milk processing, chemicals, medical care, pharmaceuticals, and others.) Both the Internet and the grid, as we shall see, were exemplary examples of efficient, decentralized, reliable networks, but are in danger of concentration. Regarding the Internet, Microsoft, allegedly through illegal anticompetitive practices, has gained 90 to 95% of the operating systems that computers use. In doing so, it is charged, it paid little attention to reliability, stifled innovations by buying up innovators that threatened it, and, having a near monopoly, did not have to pay attention to security. A report by several experts on computers and security concludes, "The presence of this single, dominant operating system in the hands of nearly all end users is inherently dangerous" (Geer et al., 2003). Microsoft's near monopoly left the Internet open to malicious hackers, who have disrupted parts of the critical infrastructure represented by the Internet from time to time, and to terrorist organizations that have expressed an interest in using the Internet as a terrorist tool, but so far have failed to do successfully do so, as far we know. Had the concentrated power of Microsoft been checked, as a federal lawsuit tried to do, but failed, there would have been more room for competitors who could have competed on the basis of higher reliability and higher security. Now, even the Defense Department has few alternatives to using insecure and "buggy" Microsoft products for its mission-critical systems. (It can get the secure codes from Microsoft and reconfigure Windows, for example, to be safer. Others cannot.)

The increasing concentration in the media industry also poses security problems. Media conglomerates are attempting to reduce the number of independent Internet Service Providers (ISPs) that are available from thousands to a handful. Access to Web pages would be limited to those the cable or DSL company subscribes to (Krugman, 2002; Levy, 2004). A system with a few ISPs is arguably more vulnerable to our three sources of disasters than a highly distributed one with thousands of points of access. (Terrorists should have no trouble breaking into and shutting down a Comcast ISP; hackers break into the more highly protected Defense Department computers almost daily, though they appear not to be disposed to shutting down vital systems. Terrorists could be so disposed.)

The most vital element of our critical infrastructure is electric power, and blackouts the most disastrous event. Deregulation appears to be the "root cause" of the August 14, 2003 blackout in the Northeast, since deregulation led to concentration in the industry. It was supposed to increase competition and drive down prices. Prices did not decline, and it did not produce the competition that would encourage greater innovations and more efficient and reliable transmission. Rather, competition among consolidated utilities was strictly in terms of profits that could be increased by cutting maintenance and requiring "the grid to be operated closer to its reliability limits more of the time than was the case in the past," according to the North American Electric Reliability Council (NAERC). It removed the incentive to add transmission lines to increase reliability, since their costs would not be reimbursed through the regulatory process as they had been in the past. Consequently, investment in transmission has lagged. Competition and consolidation in the industry, after deregulation in the 1990s, replaced the company heads, largely engineers, with lawyers and MBAs without technical experience. Reserve margins of electricity to reduce shortages have been replaced by lower margins; lower margins will drive up prices and increase profits (Wald, 2005). This was apparent in the rigged California market, where the utilities and the larger energy companies such as Enron created artificial shortages to drive up prices (McLean & Elkind, 2003).

Since electric power is the preeminent item in our critical infrastructure, the decline in reliability because of economic concentration is troubling. With decreasing reliability, terrorist attacks are more possible, and storms that disable substations more consequential. Congress deregulated the industry; it could re-regulate it. Its only watchdog, the North American Electric Reliability Council (NAERC), is a voluntary association funded by the utilities, and has no authority to require, as a prime example, the utilities to invest in new transmission lines.

THINKING ABOUT INTERCONNECTEDNESS

How can we reduce our vulnerabilities? This will certainly be difficult since it will impose costs upon business and industry, and local and state governments, and runs counter to our prevailing economic wisdom, which favors large organizations on the grounds that they have economies of scale. It would mean widespread dispersion not only of "hazmats" but of settlements in hurricane zones and flood plains as well, and the breakup of large organizational concentrations of power, or at least their decentralization. It would require a great deal more regulation than these organizations, and our Congress and governmental agencies, are now willing to entertain. But the vulnerabilities are not necessarily inherent in our society; they were less in past decades and could be reversed.

It is my argument that many, though not all, of such vulnerabilities stem from dependencies, and their reduction will be achieved by creating interdependencies. This requires that be clear about interconnectedness.

We speak loosely of a highly interdependent, networked world, but true interdependency is rather rare. Everything is indeed connected, but most of the connections exhibit far more *dependency* than *inter*dependency; more control than cooperation.[5]

True interdependency means reciprocal influence. Behavior by A not only affects B, but B's response changes A in turn. This is the normal interaction of two people with roughly equal power. When power is unequal we can still have some reciprocity, but the reciprocal effect of B on A may be small. Say General Motors asks the Quiet Door Company to bid on making a part of its door, and the Door Company gets the contract and makes the doors. The door company is dependent upon GM. But suppose the door company suggests to GM that there is a better way to design their part of the door and this will save both GM and the door company money. There is a least a small bit of reciprocal influence here. In some industrial networks, especially in Japan and northern Europe, this *inter*dependency is enlarged; for example, the supplier may participate in the initial design of the buyer's product. The supplier changes the buyer. Some industrial networks consist of firms with roughly equal power, and a great deal of interaction or reciprocity.

Reciprocal effects can occur when the interactions are programmed with self-adapting mechanisms. Take some segments of our power grids. Here, A and B are nodes in a network, and component A sends information or commands to component B, and B evaluates the information or command in terms of its view of the system's state—say its links to C, D, and E. If B does not accept the information as complete or valid, or finds the command violates something in the network at that time, it responds in a way that requires A to alter the command or expand the information to clarify it. B is not fully dependent upon A, and an instant later, B may be sending commands to A.

The Interdependency Opportunity

To an increasing degree this automatic reciprocity appears in highly sophisticated electronic systems. Over time, the components, called "intelligent agents," acquire a "memory" that guides their interpretation. Computer speech recognition programs such as Adobe Naturally Speaking are a primitive version of these responses. The program is designed to learn, making subtle decisions as to when to type "knot" instead of "not," expanding and adjusting its initial memory to respond to your tone of voice and phrasing. It must be trained. More important for reciprocity, the interaction is not solely one way. Indeed, I find I speak more clearly when I use it. My behavior is changed.

Sophisticated segments of the electric power grid show learning and collaboration, and the industry aspires to have intelligent agents deployed at critical nodes (Amin, 2001, 2002). It also occurs in the Internet, especially when packets are rerouted because of congestion. No human intervention is involved in either of these operations, and while a few nodes are much more significant than the vast majority—the organizing principle follows a "power law"—there

[5] The discussion in this section takes off from some seminal distinctions by three engineers. I have modified their scheme extensively, renamed some key variables, and introduced the notion of the difference between interdependency and dependency (see Rinaldi, Peerenboom, & Kelly, 2001).

is considerable interdependency, largely achieved through redundancies.[6] Let us call this form of interdependency "*reciprocal interdependence.*" It is to be highly valued.

A second form of interdependency, also to be valued, I will call "*commonality interdependency*," though I wish I had a better term. (It involves interoperability, but that term is usually not applied to symbols such as laws.) If two systems have different languages, metrics, or voltages, they cannot communicate. If they are governed by laws or regulations that are not shared and compatible, they cannot coordinate. If their reputations are disparate, dependency will prevail over interdependency. Nations with incompatible laws and legal structures have minimal reciprocal interdependency with each other. Police and fire departments with incompatible communication systems cannot communicate. China, with a policy of secrecy, could not alert the world to the SARS epidemic before it was too late; it did not have an openness policy in common with other nations. The Mars Lander failed because of incompatible metrics within its system. Firms with low reputations for reliability are assigned to a dependent role, if they are not simply forced out of business, as Arthur Anderson was after the Enron scandal. Commonalities may be physical, as in the case of voltages or standardized screws, but the most interesting are these "logical" commonalities.

The Dependency Problem

When we enter the world of nations, firms, and public service departments such as police and fire, or the Central Intelligence Agency and the Federal Bureau of Investigation, we should not assume a high degree interdependency, in the form of logical commonalities. As noted, while the world is getting more interconnected, the connections are increasingly ones of *de*pendency, though we may mistake this for interdependency.

There are two attributes of systems that are often cited as evidence of a society's high degree of interdependency, but should be cited as examples of *de*pendency. The first is called *physical dependency*, and occurs when a system requires a specific kind of input from another system. (The inputs do not have to be physical, but this is the most common example.) The railroad engine needs coal to operate, so it is dependent upon coal suppliers, but it is hardly *interdependent* with any one supplier. Just as the railroad is dependent upon fuel suppliers, the fuel suppliers are dependent upon railroads to buy their fuel, and we like to see this as interdependency, but no reciprocity is required; there are only two examples of dependency, both of which can be exploited.

But this dependency can be reduced if the railroad engine can burn either coal or oil, increasing the range of suppliers it can draw upon, just as the fuel company is less dependent if it has both coal and oil and many railroad customers and other users. Physical dependency is high when the railroad engine can only burn coal, lower if it can shift to oil; or high if the coal company has only one customer, the railroad, but lower if it has several customers, and lower still if the several are not all railroad engine customers. While there may be economies

[6] The sender's message is broken up into packets, and these are directed by routers to find the shortest way to the receiver, via servers. If there is congestion at a server or on the route, or a failure in delivery for any reason, the receiving machine checks a packet that has arrived for the address of the missing packet or packets and asks that it be sent again. Each packet contains not only the addresses of all other packets of the message, but a "table of contents" of the message, which provides a further redundancy. There is no cost to these redundancies; indeed, they allow packets to find the shortest uncongested route and thus increase efficiency. It is a bit of a stretch to label all this "interdependency," or "reciprocity," but it is close to that.

associated with an engine built for only one fuel rather than two or three, or a coal supplier with only one customer, there are vulnerabilities associated with single-purpose machines and single source suppliers or customers. There is a high degree of dependency, rather than interdependency. Flexible, multipurpose machines, and multifirm suppliers and customers, reduce these dependencies, and involves more multinode, complex networks, which are partially self-regulating. More important for the argument on vulnerabilities, it also results in smaller concentrations of hazardous materials and lower economic and political power for any one organization.

The flexibility and multipurpose characteristics do not necessarily create *inter* dependencies, but it greatly increases the opportunities for them. While there is some movement toward multiplex networks in a few new industries and research areas, overall we are seeing increased concentration and dependencies.

The second example of *de*pendency will be called "spatial dependency." This is similar to what engineers call "common modes," as in common mode failures. These occur when the failure of an electric power source shuts down not only the nuclear reactor, but also the cooling system in a quite different, but spatially adjacent, system that keeps used fuel rods cool while their radioactivity decays and they await shipment to a permanent storage place. The two systems, power generation and spent fuel rod cooling, need not be linked, but are for minor economic reasons. Or, if a bridge carries not only vehicle traffic but also communication and power lines, its collapse would stop not just traffic but communication and power as well. A vehicle bridge does not require telephone and power lines on it to function.

There are clear economic efficiencies associated with most spatial dependencies. It would be expensive to build two bridges. But it would cost only a little bit more to move the spent storage pool to a distant site that is not dependent upon the nuclear power plant for power. Where catastrophic failures might be experienced, as in the nuclear power case, the risks seem very high compared to the economic benefits.

Spatial vulnerabilities with catastrophic potential abound in our society. We settle on flood plains and hurricane-washed coasts with inadequate building codes and evacuation routes and build cities on known earthquake faults and suburbs on unstable bay fills. We allow unnecessarily large storage of hazardous materials in with dense population concentrations, making them vulnerable to terrorist, industrial, and natural disasters. These vulnerabilities could be eliminated or reduced through better system design that recognizes and reduces this form of dependency. (Fortunately, just-in-time manufacturing and processing practices may lead to a dispersal of some hazardous materials in smaller storage containers.)

Physical dependencies abound because of concentrations of economic and organizational power and can be reduced through reducing these concentrations. But reductions of both forms of dependency run afoul of the economic argument that economies of scale justify these concentrations.

FOUR EXAMPLES OF LARGE, EFFICIENT, RELIABLE AND DECENTRALIZED SYSTEMS

There is ample evidence that very large scales only sometimes produce production economies, but instead produce the social inefficiencies of market power and the political power that can flow from it. It is possible to have very large systems that are highly decentralized, very efficient (they have economies of network scale, rather than economies of organizational scale), innovative, and very reliable, minimizing their vulnerability to the three disasters.

Here are four examples. They are all heavily networked systems, low in physical and spatial dependencies, where the *pathologies* of networks reside, and high in reciprocal and commonality interdependency which represent the *potentials* of networking. Not everything we do in society could be organized in this form, nor is everything that involves our critical infrastructure, but there may be many systems that could be so reconfigured.

They are the Internet, the electric power grid (two essentials for our critical infrastructure); networks of small firms (most prominently in Europe and Japan, but some in the United States); and, alas, the global terrorist network associated with radical, fundamentalist Islamic religion.

We will start with *size*. The Internet is the world's largest system, embracing the globe. Nothing compares to it in terms of size. The U.S. power grid has been called the world's largest machine, reaching from coast to coast and into Mexico and Canada (though made up of three regional systems, they are connected to each other).

Networks of small firms are much smaller of course, but their output can be much larger than that of one or two large companies making the same products. In fact, typically they displace a few large firms. The point is that the small size of most of the firms in the networks is not an economic drawback, but turns out to be a virtue. They are most famously prominent in northern Italy, where an industry making machinery, scientific instruments, furniture, or textiles and clothing will range from a few dozen firms to hundreds, all interacting.[7] Finally, although reliable information is not available, it is estimated that the Al Qaeda terrorist network is made up of thousands of cells.

Our four examples point to two important size considerations: the systems can expand easily in size, and can increase in size without increasing their hierarchies, that is, without encumbering themselves with layers of managers and all the associated costs and complexities. Thousands of new users have joined the Internet every day for years. The power grid can add new lines, territories, and capacities rather easily as can networks of small firms and terrorist groups. This is associated with the "power law" distribution of nodes in these networks. While there are a very tiny number of absolutely essential nodes, the vast majority of nodes have only a few connections to other nodes, so adding them does not affect the vertical structure. But only a few connections are needed to be able to reach the whole vast network of Internet users, power suppliers, small firms or terrorists cells, so efficiency is not decreased with size. Even the criticality of a tiny number of key nodes in the Internet and the power grid is rarely a source of vulnerability because of extensive redundancies designed into these systems. In all these respects, the networks are very different from traditional organizations, such as firms.

Next, consider *reliability.* The Internet is remarkably reliable, considering its size and what it has to do. Computers crash many more times than the Internet, and Internet crashes are generally very brief (excepting deliberate attacks). The reliability of the U.S. power grid has been very high, with major outages occurring only about once a decade. It is true that there have been very serious blackouts in the United States, and "normal accident" theory would say they are to be expected because of interactively complexity and tight coupling (Perrow, 1999). But these kinds of accidents are not just rare, as normal accident theory would expect, but must be considered exceedingly rare given the excessive demands on the system and its size and complexity. Much more likely to cause failures are production pressures, forcing the

[7] There is a vast literature on this. For starters, look at the classic Piore and Sabel book that gave the notion, discovered by Italian demographers, its first prominence (Piore & Sable, 1984). It is developed in (Lazerson, 1988). For a synthetic overview, see (Perrow, 1992). For more recent extensions, see Amin (2000) and Lazerson and Lorenzoni (1999).

system beyond design limits, and of course deliberate destabilization to manipulate prices, as in the Enron case in California.

Between 1990 and 2000 the U.S. demand increased 35% but capacity only 18% (Amin, 2001). One does not need a fancy theory such as normal accident theory to explain large failures under those conditions. (Indeed, one does need a fancy theory, such as a network theory that gives a role to interdependencies and redundancies, to explain why there were so few failures under these conditions.) One failure in 1996 affected 11 U.S. states and 2 Canadian provinces, with an estimated cost of $1.5 to $2 billion. Even more serious was the 2003 Northeast blackout. Since the extensive deregulation of the 1990s we can expect more failures as maintenance is cut and production pressures increase. But I am struck more by the high technical reliability of the power grids than by the few serious cascading failures it has had in some 35 years. Without centralized control, despite the production pressures of mounting demand, and despite increased density and scope, it muddles through remarkably well, if it is not manipulated by top management and banks.

The reliability of networks of small firms is more difficult to assess, since there is no convenient metric. But students of small firm networks attest to their robustness, even in the face of attempted consolidations by large organizations. Saxenian effectively contrasts the decline of the non-networked group of high-technology firms around Boston's Route 128 when federal funding declined and Japanese mass production techniques matured, with the networks of small firms in California's Silicon Valley, who charged forward with new innovations for new markets (Saxenian, 1996). Despite predictions of their imminent demise (Harrison, 1994), dating back to the 1980s when they were first discovered and theorized, the small firm networks of northern Italy have survived. In the United States the highly networked biotech firms are prospering, for the time, despite their linkages with the huge pharmaceutical firms (Powell, 1996). Particular firms in small firm networks come and go, but the employees and their skills stay, moving from one firm to another as technologies, products, and markets change.

The reliability of terrorists' networks also seems quite high. Rounding up one cell does not affect the other cells; new cells are easily established; the loosely organized Al Qaeda network has survived at least three decades of dedicated international efforts to eradicate it. There are occasional defections and a few penetrations, but the most serious challenge to it has been the lack of a secure territory for training, once the Taliban was defeated in Afghanistan. (Some argue that Al Qaeda per se is increasingly just one part of a leaderless network of Islamic terrorists.)

Can huge, decentralized networks of small units be *efficient*? It appears so. The Internet is incredibly efficient. Power grids are becoming more so as they add "intelligent agents" (though the concentration of generation and distribution firms reduces maintenance and thwarts needed expansion of the grid). Small firm networks routinely out-produce large, vertically integrated firms. Network economies of scale replace those of firm size, and rely, in part, on trust and cooperation, allowing strong competitive forces only when the overall health of the network is not endangered. Transaction costs are low and handled informally. And finally, terrorist networks live off the land, largely, can remain dormant for years with no maintenance costs and few costs from unused invested capital, and are expendable.

I have tried to establish that decentralized systems can be reliable and efficient, but does it follow that the systems responsible for our basic vulnerabilities could be organized like this? The Internet already is, though that is changing. The security vulnerability of the Internet, making it open to terrorist attacks, could be greatly reduced, for instance, by making providers such as Microsoft liable for having a code that is easily "hacked." The electric power grids will remain reliable if maintenance and improvements are required, which could be done through legislation and liability legislation. Deconcentrating industries that deal in hazardous materials, such as petroleum and chemical industries, could greatly reduce vulnerabilities there (heavy regulation would also be needed), and the power the firms would lose would be market power. Without market power they will be more sensitive to their accident potential. Research and development, which might need large amounts of capital and might have to be centralized, could be detached from production, storage, and delivery, which could be decentralized. Population concentrations in risky areas is not a "system" that could be decentralized along the lines of our four examples, so in this case the reform must depend upon regulations and improvements in the insurance and liabilities area (e.g., stop federal subsidization of disaster insurance; allow federal aid only if federal standards have been met; increased inspection and penalties; etc.). None of this would be easy, but none of it is inconceivable.

In every case of vulnerabilities I have mentioned, we have had laws and regulations that address these issues, but they have been dropped, weakened, or are not enforced. Take a trivial example. The government has tried to withhold disaster relief from those who failed to take out subsidized insurance or failed to conform to regulations, but it has backed off when the flood or hurricane actually came. This could be corrected. More important, we have precedents for deconcentrating organizations; 30 years ago we had effective antitrust legislation; it could be reinstated. We tried to break up Microsoft; we could try again. It doesn't even produce many innovations on its own; it has the market power to buy them up. We could once again regulate the Internet as a common carrier.

Unfortunately, we appear to be moving in the opposite direction. The power of Microsoft to shape computing and the Internet does not seem to have declined, but to be increasing. It is gaining control of the new technologies such as the Internet, browsers, and music that were supposed to check its power. Concentration in the electric power industry is proceeding apace under deregulation. Even networks of small firms may prove to have had only a half-century of efflorescence, as giant retailers control the "commodity chain" that forces producers into mass production in low-wage countries where exploitation is easy and the only alternative to workers is rural starvation.

All of these developments will make us less safe because they will increase our vulnerabilities to natural, industrial, and deliberate disasters.