DISASTERS EVERMORE? REDUCING OUR VULNERABILITIES

Charles Perrow, Department of Sociology, Yale University  8/26/2005

After April 14  Mail proofs to 135 Cliff St. New Haven, CT, 06511

203 562 3848 phone  203 562 6779 Fax

(Contact until April 14:  560 831 1923 – no fax -- (14 Morton way, Palo Alto, CA 94303))
Natural disasters, unintended disasters (largely industrial and technological), and deliberate disasters have all increased in number and intensity in the last quarter century.¹

Figure 1 lists some examples and some causes. Our typical response has been remediation (recovery), limiting the damage, and prevention. 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 et al. 2003) Furthermore, we have a “panic” model of behavior, which mistakenly limits information, which in turn breeds skepticism on the part of the public. The panic model also legitimates another unfortunate tendency: the centralization of responses, whereas research shows the most effective response comes when 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 protection of hazardous materials, and evacuation plans. There has been improvement here, but not enough. We still subsidize the potential losses of people who settle in risky areas and make few demands upon them to pay a fair share of the levy upon the rest of the population. Real estate interests resist higher standards and limits on settlements, the government subsidizes insurance and bails out those who refuse to take it. This area of disaster management is full of perverse incentives.

Finally, preventing damage is the most developed, since there are profits to be found in prevention devices. Here we have alarms and warning systems for natural and industrial dangers, and detection and encryption to protect ourselves from terrorists. The economic opportunities are substantial. As soon as the Department of Homeland Security 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 that registered and listed “homeland,” “security,” or “terror” on their forms was already
sizeable 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 on-line resume that he authored a newsletter article titled “Opportunity and Risk: Securing Your Piece of the Homeland Security Pie.” (Shenon 2003; Shenon 2003) It is a very large pie indeed.

Also in the prevention area are inspections, surveillance, and border controls to prevent terrorists and weapons of mass destruction from entering the country. These have expanded greatly, but seem forever inadequate to the task.

The most promising response, to reduce vulnerabilities to all three sources of disaster – natural, industrial, and deliberate -- rather than to just limit, prevent or better recover from them, is the least considered by policy makers (though it is recognized in the academic disaster literature), and it is what I will focus upon. 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.

• The second are concentrations of populations (in risky, though desirable areas), and 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, and in the Internet (e.g. the “monoculture” Microsoft has created).

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 not only widespread dispersion 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 governmental agencies, are willing to entertain.

Despite the difficulties of reducing basic vulnerabilities to the three disaster sources I would like to explore some notions that might allow us to analyze the problem more clearly. We will always be vulnerable to natural disasters even if our climate were not changing and new epidemics not emerging. Industry will forever be subject to a range of errors, by workers, managers, designers and so on, since nothing is perfect or risk free. And the U.S. has produced a respectable crop of domestic terrorists over the last century and will continue to do so, even if the much greater threat of Islamic terrorism did not exist. (The latter appears to be growing, rather than leveling out or declining.) In view of all this, while we need more and better programs for remediation, limiting damage, and prevention, we might also explore the additional, more fundamental, strategy of reducing basic vulnerabilities. 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.

**Thinking 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 interdependency; more control than cooperation.

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 at least a small bit of reciprocal influence here. In some industrial networks, especially in Japan and northern Europe, this interdependency 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.

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 like Adobe Naturally Speaking are a primitive version 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; Amin 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 is considerable interdependency, largely achieved through redundancies. 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. 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; our “global economy” is largely one of dependency relations. 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; they 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 a 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 CIA and FBI, 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 dependency, 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 dependency. 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 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.

These vulnerabilities loom large when the nation’s critical infrastructure is examined. As noted, it is vulnerable to natural disasters, industrial disasters, or deliberate disasters such as terrorism. But it is not the so-called interdependencies that make our critical infrastructure vulnerable to these three sources of disasters. It is the dependencies in the nation that should be our concern. Flexible, multipurpose machines, and multi-firm suppliers and customers, reduces these dependencies, and involves more multi-node, 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 multi-purpose characteristics do not necessarily create interdependencies, but it greatly increases the opportunities for them. While there is some movement towards multiplex networks in a few new industries and research areas, overall we are seeing increased concentration and dependencies.

The second example of dependency 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 a electric power source not only shuts down the nuclear reactor, but shuts down the cooling system needed to keep the spent fuel rods from fissioning. The two systems, power generation and spent fuel cooling, need not be linked, but are for minor economic reasons. Or, if a bridge not only carries vehicle traffic but 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; 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 thru reducing these concentrations. As a result of deregulation, the electric power industry is concentrating and this, it can be argued, lay behind the Northeast blackout of 2003. The lack of security of our Internet can be traced to the near monopoly power of Microsoft. 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

I think there is ample evidence that very large scales rarely 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, are very efficient (they have economies of network scale, rather than economies of organizational scale), are 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 represents the potentials of networking. Not everything we do in society could be organized in this form, nor 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 firm (most prominently in Europe and Japan, but some in the U.S.), 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. Finally, while 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. So 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 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 U.S., 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 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 1990’s we can expect more failures as maintenance is cut and production pressures increase. But I am more struck 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 immanent demise, dating back to the 1980’s when they were first discovered and theorized, (Harrison 1994) the small firm networks of Northern Italy have survived. In the U.S. the highly networked bio-tech 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 become 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 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. Deconcentrating industries that deal in hazardous materials, such as petroleum and
chemical firms could greatly reduce vulnerabilities there (along with heavy regulation), 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 I have mentioned of vulnerabilities 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; thirty years ago we had effective anti-trust 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 efflorescence, as giant retailers control the “commodity chain” that forces producers into mass production in low wage countries where exploitation is easy and preferable to rural starvation.

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


**FIGURE 1**

**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)
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 U.S., 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 1970's 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 1970's and early 1980's, there was a decline. But there has been a rise in the 1990's to the present.

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, S. M., J. P. Peerenboom, et al. (2001). "Critical infrastructure interdependencies." IEEE Control Systems Magazine.

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 not only contains 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.