Organizationally Induced Catastrophes

C Perrow

May 29, 2000

The extreme events I will be concerned with are those that are human in origin, organizationally induced, with catastrophic consequences, that is, either death or serious damage to hundreds of people or environmental destruction over large areas. The principle agent of these events are large organizations, though some extreme events have non organizational beginnings, but are aided by large organizations, such as the spread of epidemics. [The role of organizations in my category, organizationally induced catastrophes, will be roughly categorized as (1) prosaic organizational failures, the most frequent; (2) unintended consequences of successful operations, quite rare; and (3) rare but inevitable failures associated with complexly interactive systems with tight coupling. Policy considerations will include cost/benefit ratios, and the difficulty of producing catastrophic events from failures of whatever cause.] My most general point is that organizations in relatively unregulated markets will move towards more catastrophes despite efforts to increase safety, and the main reason for this is increasing size and scope of organizations. [By size I refer to market control, and the number of employees and sales, for the for-profit organizations, and in the case of not-for-profit and governmental organizations, the amount and variety of services. Scope entails the variety of goods or services, and usually correlates with size.]

The importance of size is extensive. Catastrophic failures are the uncontrolled and unwanted releases of energy to the organization and the environment. The larger the organization the more energy is available for release. One thousand organizations, each producing one unit of desired output, but inadvertently releasing one unit of uncontrolled energy, will have much less effect than one organization producing one thousand units of desired output that inadvertently releases one thousand units of uncontrolled energy. The consequences are not dispersed over space and time, but concentrated. The release is likely to disable the large organization, whereas it probably won't disable all the small ones. The concentrated release has more possibility of causing the failure of other systems in the environment than releases dispersed over time and space.

Furthermore, there is more potential for failures, that is, unwanted and uncontrolled releases of energy, in very large organizations than in many small ones that produce, in aggregate, the same output as the large one. While the large

organization will presumably generate more slack resources – those not needed for production – than small ones, and thus can invest in safety devices, it will need more coordination and control than the small organization, thus absorbing much of this slack. Each time a supervisory level, or another production unit is added, some staff time and some physical resources have to be devoted to problems of coordination and control that do not arise in the organization without the extra level or unit. Slack is also absorbed in the large organization through the inevitable development of group interests, wherein personnel have invested in relationships and routines and procedures that will make their world more comprehensible and their work easier or more pleasant. The more personnel, the larger this small extra "charge" to production, and the less slack available for safety considerations, including drills, warning devices, maintenance, firewalls, redundancies and the like.

Nevertheless there are cases where small is more risky than large. Small airline companies have more failures per take-off and landing than large ones. The slack in the large ones, whether produced through efficiency or through market control and regulatory capture, enables them to buy the latest equipment, and accident rates decline dramatically as each new generation of aircraft is introduced, despite the fact that the newer generations can be flown in more hazardous conditions. However, they also carry more people and release more energy to the environment when they fail. [While African airlines have about 8 times the accident rate of US airlines, per take-off, the risk to the total population of Africa is probably less than the risk of accidents of US airlines to the US population. Still, air transport does not support my generalization about size and failures.] But Smaller is riskier for airlines.

The generalization that big is more risky is supported for most other risky systems, however. Large shipping firms appear to have similar spillage rates of small quantities of oil as small ones, rather than less, and the large firms certainly have more catastrophic spills. Even regulation does not seem to make much difference here; Exxon was more regulated than the hundreds of firms that have not had catastrophic failures and operate under less strict regulations. In the chemical and petroleum industries there appears to be a strong correlation between major fires and explosions and the size of both plants (as one might expect, of course) but also with the size of the companies. One careful study of excessive emissions of U.S. chemical plants found that "big was bad." Fires in large cities kill more by any measure than those in small cities. Though it is not really a human generated catastrophe, epidemics do more harm in large cities than small ones and the

countryside, and depend upon organizationally based transportation routes. With some exceptions, then, we can argue that organizational size and catastrophes are positively related. More important, this is not a circular argument. Small organizations have the potential to release large amounts of energy catastrophically, but do not seem to do so as often as large ones. The reasons are organizational.

The most common cause of organizational failures, and it is the most simple and obvious, is what I have termed "component failures" or prosaic organizational failures. The component that fails can be the design, equipment, procedures, operators, supplies and materials, or the environment (abbreviated as DEPOSE factors). Everything is subject to failure, and if the failure of one of these factors is large enough, it can bring down the system. A component failure seems to be the cause of such accidents as Chernobyl, Bhopal, the Challenger, and the Exxon Valdez. Component failures do not seem to be more likely in large than small systems, though the consequences will be greater in the large systems. We understand the potential of all components to fail, so we build in numerous safety devices, such as alarms, buffers, redundancies, design testing, operator training, and employee punishments and rewards. Some theorists believe that with sufficient – actually overriding – attention to safety, even the most complex and tightly coupled systems can be virtually disaster free; this is called the High Reliability school, asserting the possibility of High Reliability Organizations. But two considerations greatly limit the possibility of failure-free organizations. [(Actually, failures are expected, but safety devices will limit the damage, so this should be termed "system failure-free organizations," to signify that recovery without significant damage to the system is possible.)]

The first consideration is a rather obscure and preliminary formulation: one report on oil refineries points out that it appears that if the system is sufficiently complex (an enormous number of nodes connecting things) everything may work just fine, but under some (presumably rare) combinations of interactions there can be a failure simply because no designer (let alone operator or monitor) could have anticipated this set of combinations. Because of the tight coupling of refineries (no slack, no way to reverse or stop a process, no substitutions possible, etc.) the failure will cascade and bring down the system or a major part of it. Subsequent investigations will not reveal the cause of the failure and make similar failures unlikely because nothing actually failed, though one might say the designer failed to take everything into account. I do not want to make too much of this "*overwhelming complexity*" failure, as it might be called, but there are some possible instances. In a

city such as 19th century Chicago where buildings were dense and made of wood, the normal provisions for putting out unwanted fires could be overwhelmed by the proximity of other flammable structures, and while the fire-fighting provisions operated as required, they were insufficient under the particular configuration of structures and direction and force of the wind. A massive fire destroyed much of the city. I would expect that as global financial flows become more and more dense, everything might be working as designed, but the design did not anticipate the number of nodes in the financial system and the possibility of overloading some channels.

More likely, or at least I have located and discussed dozens of instance that seem to fit in a review of accidents in risky systems, is what has come to be called the "normal accident," or what I designated as a "system accident." Here interactive complexity allows the possibility, rare though it may be, that two or more failures – and remember, nothing in the DEPOSE factors can be free of failure – two or more failures interact in such a way as to defeat the safety systems designed to accommodate individual failures. A sizeable failure results as the combination of two or more failures, perhaps quite trivial ones singly. If the system is also tightly coupled operators will not be able to intervene in time to prevent a cascade of failures. The poster-boy accident of this type is the one at Three Mile Island, where four small failures interacted unexpectedly and led the operators to zig when they should have zagged. They did what their training told them to do. Two failures were on the "hot" side of the plant, and two on the "cold" side, making their interaction mysterious. Three of the four had occurred before without undue harm, and the fourth was a new safety device introduced because of earlier problems with a failure. It just happened to fail too. The actual sequence of events, occurring over about 90 seconds, was incomprehensible to the operators – indeed, it took considerable study to understand it later, and some argued that zigging rather than zagging was indeed the best thing to do after all. (Nevertheless the Presidential Commission still blamed the operators.) [It would take too long to walk you through the accident, though I have brought the materials with me in case there is some gap in our schedule and you are interested. It is a rather gripping tale, as are many of the "normal accidents" I covered in my book.]

Two subjects remain. Why do we keep building risky systems if experience tells us they have catastrophic potential and have occasionally realized that potential? And, is it possible that as organizations grow larger and more

interdependent that we will see more accidents, no matter how hard we try to prevent them?

A couple of years after I published *Normal Accidents*, we had the Bhopal disaster in India, and I was struck by the fact that with some 40 years of hundreds of chemical plants with the toxic potential of Bhopal, this was the first major disaster. This allowed me to kind of invert Normal Accident Theory and note that it takes just the right combination of a number of circumstances to turn an accident into a catastrophe. As I had noted in my book, one of the most commonplace comments after accidents is "we are lucky it wasn't worse."

Clouds of lethally explosive gas had been known to drift over sleeping suburbs, but dissipated without being ignited because there was no automobile traffic late at night. The potential for a catastrophe was there. Other clouds in sparely settled areas did find ignition sources but few people were around to be killed. Most potentially catastrophic accidents kill only a few people, as the one in Flixborough, England, 1974, which occurred on a weekend when the chemical plant was only lightly manned, and the people in the adjacent community (where buildings were severely damaged) were away at a nearby market town. At Chernobyl, had the wind been blowing toward nearby Kiev and the weather been soggy, the full course of the radioactive materials would have drenched that city of two million. The Exxon Valdez went to ground on a clear night with tiny waves and little wind; if it had been stormy it could have been much, much worse. The Grand Teton Dam failure was massive, but there was an hour and a half warning, and few perished. The Vaiont, Italy, dam failure had no warning and three thousand people perished. There are only two cases in the history of air transport where the airplane crashed into a tall building filled with people (and there were few casualties), and tall buildings have frequently gone up in fire or suffered extreme dioxin contamination as the result of wayward equipment, but few people happen to have been in them.

But he Union Carbide plant at Bhopal had several of the right conditions for a major catastrophe. At Bhopal there was no warning, no evacuation plans, no alarms, people were in their houses and asleep, and a light wind brought the deadly gas right to the people. Absent any one of these and the toll might have been a hundred rather than thousands. The U. S. Environmental Protection Agency estimated in 1989 that in the U.S., in the previous 25 years there were 17 releases of toxic chemicals in volumes and levels of toxicity exceeding those that killed at least 4,000 in Bhopal. But mostly because of what we are disposed to call "sheer luck" only 5 people were killed in those accidents. (Shabecoff 1989) It is hard to have a

catastrophe; everything has to come together just right (or wrong). When it does we have "negative synergy." Since catastrophes are rare, elites, I conclude, feel free to populate the earth with these kinds of risky systems.

[Though rare, do they very by political systems? Certainly Soviet socialism has one of the worst records for all kinds of disasters. But the record for Europe, and especially for northern Europe seems to me to better than our own. Regulation tends to be more effective, and the size of units is generally smaller.]

Will organizationally induced extreme events increase in number and extremity? It is possible to argue both ways. We have reduced the number of nuclear weapons in the world, and neither the former Soviet Union countries nor the U.S. is on the high level of alert that we once endured. But a recent article in the Bulletin of Atomic Scientists documents shocking conditions in our nuclear weapons facilities, with several catastrophes just waiting to happen. Our nuclear power plants appear to be safer than they were before TMI, but there is recent evidence that the NRC is reverting to a "self policing" policy and reducing inspections, and the deregulation of the electric power industry will result in less concern for safety in the nuclear plants. Terrorist threats have reportedly been increasing, prompting more focused governmental activities and even the establishment of a "terrorist czar" in the government, following a special presidential panel's recommendations regarding the protection of the national information infrastructure. Yet the actual acts of terrorists are fairly crude and limited, and the federal concern is sometimes dismissed as overkill or bureaucratic enhancement.

Only in the private sector can we find clear evidence of an increase in serious accidents, in industrial activities and transportation, despite more sophisticated safety devices and increased awareness of environmental damages. [But so has the level of activity increased, with more chemical plants and more airplanes, so the question is, more accidents relative to what?]

I believe that there is one sizeable cloud in the sky, representing organizationally induced catastrophes, but it is highly speculative. Take two systems with the same output, one made up of many small and independent units, and the other with a few large units that are dependent upon one another. The possibilities for unexpected interaction of failures in the latter is greater. The small unit system will have enough unexpected interactions to produce failures, though somewhat fewer than the large unit system, but the failures will not propagate far because the intensity of linkages declines rapidly as the failure moves out from the initial unit to subsequent ones. Independence of units is a buffer. Only if there is a domino effect -

- units dependent upon each other -- will the failure propagate, and it is easy to limit this effect through buffers, though it was not in the case of the Chicago fire; that was a highly vulnerable unbuffered system with high proximity.

A system may be very large, but with poorly integrated units. The soviet system is an example. The lack of tight connections between, say, industry and agriculture, or industry and defense, or even education and government, limited the possibilities of a failure in one unit having much of an impact upon the other. While the system had very many component failures, I suspect it had few system accidents due to its unintegrated character. In contrast, the U.S. is moderately integrated with large units, and both the integration and the size of units is increasing. For example, the travel and vacation industry depends upon a 9 month college calender, and these industries, rather than professors, opposed efforts to have colleges operate on a 12 month calender. Or, education is both being privatized, replacing citizenship goals with efficiency goals, and integrated with business and industry, who are providing an increasing proportion of post high school training and affecting the curriculum of grade schools and high schools. This can lead to a bifurcation of the educational system. A minority of citizens will be trained for skilled positions in the economy, with a decreasing emphasis upon training for citizenship; and a larger and larger proportion will receive minimal training, leading firms to either automate to eliminate low skilled jobs or outsourcing the jobs to low wage countries. The increased coupling of business, education, and for-profit education, produces schools that serve primarily to reduce the unemployment rate by keeping most people out of the labor market while training the few skilled and professional workers that are needed. In the past, when business and industry were composed of smaller unit, and when school systems were also smaller and more diverse, (this was before extensive urbanization and population growth), there was less interaction between business and education and little for-profit education. The private sector had to content itself with schools that emphasized citizenship training more than now, and that were less stratified, in terms of social class. The present situation invites increased bifurcation of the population with the possibility of extreme events in the form of extremist politics, radical movements, and social unrest.

A danger with large units is the complexity of the unit; there is a greater potential for unexpected interactions in one big unit with 5,000 employees than in ten separate units of 500 each. Big units by themselves can produce extreme events, such as industrial or military accidents. But a failure in a large unit has consequences beyond the unit because large units are increasingly, and necessarily,

interacting with other large units. They have no choice; their suppliers, customers, vendors and even their regulators, if there are any, are also big.

The interaction of failures among units can be unexpected. For example, on a hot summer evening Consolidated Edison had too much demand for electric power; by design it relied upon AT&T at such times to use their own diesel powered generators rather than Con Ed power; but a switch failed and the diesel generators did not come on; the failure at AT&T went unnoticed because employees were at a safety meeting (downsizing had reduced the number available for monitoring) and the backup batteries went dead. Without the backup batteries it was not possible to start the diesels, so it took a long time to restart the system. This left air traffic controllers in the NY area without contact with airborne aircraft for several hours. Fortunately an additional ingredient for a disaster was not present: there were no storms in the area so the planes could see one another while diverting to other airports or gingerly landing.

Large organizations depend upon each other as suppliers and customers, and as political and social allies. Consider a large chemical plant producing the means to genetically engineer plants or foodstuffs, which are sold to a large grain or meat producer, and one or both are financially tied to mining interests in a third world country, which offers, through political connections, a large site to test out the genetically engineered products, with few safeguards. The chances of the unexpected interaction of two or more failures in the chemical product, the food producing operation, and the physical and social environment of the test area, are greater than would be the case if there were only small companies and small areas, with transparent interactions and the easy buffering or isolation of failures. One can imagine similar scenarios with world-wide financial flows. It is a commonplace observation that both economic concentration and economic and social interdependencies are increasing. It seems apparent that this can increase the risk of extreme events. I have tried to indicate some of the mechanisms that may be involved – the unexpected interaction of failures and tight coupling both within units and between units – in producing some of these events, and to indicate that regardless of these mechanisms, organizational size itself will generate component failure accidents, overwhelming complexity accidents, and normal accidents within the unit, and finally, in systems with few very large units another level of danger appears, the unexpected interactions of large units with each other.