Chapter 10

Society's Dependence on Information Systems

Contents

Chapter 10
Society's Dependence on Information Systems

Introduction

The nature of risk is being changed by much of the new high technology on which modern society depends—jumbo commercial airlines, nuclear powerplants, oil supertankers, or large computer-based information systems. In general, because new technologies can be designed to operate more reliably than the ones replaced, the risk that any particular mechanism may fail has been reduced. However, should an accidental or deliberate disruption occur, its cost can be much larger, even catastrophic. Furthermore, when society becomes highly dependent on the reliable functioning of single integrated technological systems or small collections of such systems, the possibility of a "domino-like" collapse of several of the individual connected units could also be disastrous. The failure of the Northeast power grid in 1965, which blacked out much of that section of the United States including all of New York City, is an example. [1]

Integrated systems are often created by information technology. There has been a strong historical trend toward connecting components over communication lines to form complex distributed systems, while at the same time computers have become smaller and more dispersed. In OTA's examination of future technology (see ch. 13), it was concluded that this trend toward integration would continue, driven by the effort to make information systems more convenient and more efficient.

When examining technologies such as electronic funds transfer (EFT) systems, widely available electronic mail service (EMS), and other large extensively used information systems, the following should be taken into consideration.

- The ways in which public policy can help to allocate and balance the risks society may encounter from national information systems against the benefits it may receive, under conditions where failure rates appear to be relatively low but potential losses may be high should a failure occur.
- The ability of society to retain the option to end its dependence on a particular information system if it has unanticipated undesirable effects; in other words, to avoid the possibility of becoming "locked in" to the use of certain information systems once they are installed.
- The capability of providing alternatives to persons or institutions choosing not to accept perceived risks in a new information system.
- The ways in which technology can be utilized to reduce the risks, for example by introducing additional system redundancy (alternative paths between points in the system, distributed data bases, backup computers). The risks inherent in U.S. dependence on a nationwide, interconnected telephone system (which itself is rapidly being computerized) are mitigated to a degree by the large number of switching centers and parallel trunklines.

[1] Rob Kling, "Value Conflicts and Social Choice in Electronic Funds Transfer Systems Developments, *Communications of the Association for Computing Machinery, vol. 21* No. 8, August 1978, pp. 642-657.

Failure

Large complex information systems contain millions of logical connections and are controlled by programs that themselves can be composed of millions of instructions. Consequently, it is difficult to calculate their reliability and to predict the failure rate of any particular part of the system, as well as the effect of a failure on the operation of the entire system. A further complication is that when a major failure does occur, it is often caused by a rare combination of multiple breakdowns of components. It is currently not possible to incorporate all of these probabilities into a single characterization of system reliability.

This failure problem is illustrated by a recent breakdown of the ARPANET, a nationwide packet switched network intended to be and normally regarded as highly reliable.

- The network's builders recognized that component failure is inevitable in any system and designed the network to be tolerant of such failures. The approach taken was to design the network's traffic control algorithms so as to isolate each failure to the processor or other system element in which the failure first occurred.
- The overall success of these algorithms and the software that embodies them is borne out by the rare occurrence of failure conditions that affect any significant portion of the network.
- But a recent failure did occur in the traffic control software itself–the very mechanism intended to minimize the spread of failure. Bad data in one processor was rapidly and systematically propagated throughout the network, bringing traffic to a standstill. Under normal conditions such propagation is necessary and desirable to allow the network to keep track of its current condition. Unfortunately, the propagation of false data, like poison, proved fatal. Thus, the network's primary shield against failure proved to be its Achilles heel.

This example demonstrates how difficult it is to design large and complex systems which are also reliable. Nonetheless, in many situations a distributed system such as ARPANET may be much more reliable than a centralized system of the same size, because of the distributed system's potential for isolating and therefore surviving local failures without a total system breakdown.

Little data exist from which to calculate failure probabilities because of the newness of information technology and its low failure rate. In addition, each system is uniquely designed for its purpose; therefore very little useful experience has been accumulated that would be applicable to calculating the probability of the potential failure rate for large complex systems in general.

The problem of estimating risks under conditions characterized by an uncertain but very low probability of failure and by a very high potential cost of failure has stimulated a burst of new research in risk analysis. The National Science Foundation has initiated a program of research that should contribute to improving the ability to calculate more accurately risks for large systems over the long term.

In addition, attempts are being made to design so-called "robust" systems. These systems have very high reliability, can diagnose failure, and in some cases can even replace failed components by switching to alternative ones. The message-switching computers that are custom-designed for use in the telephone network employ some of these techniques to achieve very high reliability, as do on-board spacecraft computers where long-term reliability is crucial.

It is difficult to carry out risk analysis for integrated information systems for the following reasons:

- Their *complexity,* which makes some design errors inevitable but also makes accurate estimations of system reliability very difficult.
- The *speed of computers,* in which millions of transactions are processed every minute, makes human monitoring virtually impossible. Consequently, system failures can quickly drive the system to a worst-case collapse before any human intervention can take place. This criticism was made during the congressional debate on the antiballistic missile system. It was argued that a system malfunction could fire the missile before any human intervention could detect the error and cancel the action.

  An automated national stock market or centralized check clearing system could also be subject to such catastrophes. Banks or brokerage houses could be ruined in a matter of minutes, long before it was discovered that the system had failed. The potential victims would be the owners of the failed system, individuals with accounts, correspondent organizations, and, were the failure to cascade through other institutions, even all of society.
- *Centralization of data* which occurs in many large information systems and is partly motivated by the higher security possible with a centralized system. Even if failure rates continue to be as low as predicted, this concentration would greatly increase the size of a potential loss should the very rare event occur.
- *Interconnection between systems* increases their vulnerability to failure by introducing another element, while at the same time providing a connecting path through which a failure at one node can spread to others, as was the case with the power blackout referred to earlier.

  A large, nationally networked information system may provide more day-to-day security by supplying instant backup to nodes that may fail. However, there may be also a greater risk that the entire system will go down in the event of an unlikely or unexpected combination of events.
- *Societal dependence* on the uninterrupted operation of large information systems will increase along with potential societal loss from their failure. The development of these systems is being motivated by the need for assistance in managing the increasingly complex activities of U.S. society and its organizations. These systems then become integral parts of the processes–central to their operation–rather than merely tools.

  This evolution to dependency can be seen already in the reliance of safe public air transport on the continuous operation of the computerized air traffic control system. In the commercial sector, large stores and banks rely on the smooth uninterrupted operation of their centralized computer systems. Future EMS and EFT systems will likely create similar societal dependencies much larger in scale than current examples.

It is not hard to project into the 1980's and envision the potential damage that could be caused by the failure or misuse of such systems as they grow larger, more complex, and more centralized. Some of the risks may be *physical* as in the air traffic control example or with a computerized nuclear reactor safety system. Others may be in the form of *economic* losses, such as the failure of an automated check clearing system or a national automated securities market. Still other risks may be *social,* as would occur if the larger data systems such as the National Crime Information Center or an EFT payment system were misused by the Government or by private concerns to exert undue control over individuals.

Issues

Underlying all of these concerns is the realization that although the probability that any catastrophic event will occur may be low, the potential social cost of such an event can be extremely high—even a threat to national security. This problem of social vulnerability is crucial to many issues that Congress will be addressing relating to information systems.

Specific Systems and Threats

Congress is already confronting these larger social vulnerability issues in the context of particular information systems:

- The air traffic control system has reportedly failed several times, leading to pressures for a new improved system. Possible new systems are being assessed by OTA.[2] An important but difficult question is the degree to which any new system improves reliability.
- Press reports have suggested that the Defense Department's WWMCCS* command and control system is unreliable, particularly when fully loaded under crisis conditions.[3]
- An article in the Washington Post suggests that the defense communication system is highly vulnerable, not only to full-scale nuclear attack, but to sabotage by terrorist groups.[4]

This last instance is the social vulnerability issue carried to the extreme, the vulnerability of a U.S. defense communications network to hostile attack. However, the line demarcating information systems that are vital to national security is difficult to draw, for it may include major civilian domestic systems.

Ever since Soviet interception of U.S. domestic telecommunications was reported, the executive branch has been working toward securing civilian government communications. They have also been concerned with the national security threats to domestic private communications, but the development of a policy has been slow and difficult due to the need to avoid substantial Federal intrusion into the private sector.[5]

Events over the next decade, such as a chilling of relations with foreign adversaries or an increase in domestic terrorism, would focus congressional attention on the vulnerability to attack of nonmilitary facilities such as EFT, EMS, or civilian government data systems.

Calculating Risk

Aside from the national security question, however, Congress will need to consider the societal risks inherent in new information systems. The concern about risk will lead Congress and other policymakers to search for more flexible information technologies to implement, whose failure will not be so devastating to society. Such systems, if they can be developed, may appear to be less efficient or to cost more in the short run, but would reduce the overall vulnerability of society to catastrophe.

Assignment of Risk

In deciding how to define an acceptable risk, the extent to which American society as a whole will or should accept responsibility for losses incurred due to massive failures of information systems must be taken into consideration.

---

[2] U.S. Congress, Office of Technology Assessment, *Assessment of the Airport and Air Traffic Control System,* in progress.

*An acronym for the *World Wide Military Command and Control System.*

[3] William J. Broad, "Computers and the U.S. Military Don't Mix," Science, vol. 207, Mar. 14, 1980, pp. 1183-1187.

[4] Joseph Albright, "The Message Gap in Our Crisis Network," *Washington Post,* Oct. 19, 1980, pp. Cl, C4.

[5] G. Lipsound, *Private and Public Defenses Against Soviet Interception of U.S. Telecommunication: Problems and Policy Points* (Cambridge, Mass.: Harvard University Center for Information Policy Research, 1979).

In the case of EFT, for example, the question might be whether the Government should insure liability against a major system collapse beyond the level currently provided by the Federal Deposit Insurance Corporation. A national automated securities market would raise similar problems.

When such losses have an extremely low probability, the difficulties associated with assigning risk can be easily put aside. The implication is that the policy decisions will be made on an ad hoc basis only after a failure has occurred. However, the political climate immediately after a major technological failure may not be amenable to making policy that would be sound over the long term and applicable to new events.

Management of Risk

A case can be made that much current Government regulation represents an attempt to manage risk in order to reduce hazards from consumer products, from drugs, from the workplace, or from the natural environment.[6] If national information systems create significant social risks, and if Congress chooses to attempt to mitigate those risks, several possible mechanisms or mixes of mechanisms are available for consideration.

- *Regulation:* Direct management through laws and administrative rules is currently being questioned as an effective means to regulate risk. For example, direct regulation was rejected by the Privacy Commission as an approach to the privacy problem. However, in specific sectors where the industry is already federally regulated, such as banking or securities exchange, Government may choose to directly set policies for protecting information systems.

  The Government is establishing standards for secure design of systems used by Federal agencies. While these standards do not apply directly to the private sector, they could provide incentives for similar design, either by setting a favorable example or by establishing a minimum standard of practice that the courts might recognize in liability suits.

Alternatives to regulations may also be considered. Two that have been proposed are:

1. *Liability:* Liability law is the chief risk deterrent through the legal mechanisms available, e.g., lawsuits.
   - Liability case law is very slow to develop, depending as it does on an accumulation of court decisions and appeals.
   - The message sent to organizations through court decisions can be vague and difficult to interpret. Thus, an unnecessarily conservative approach may be inadvertently encouraged, and promising socially desirable technological innovations may be precluded.
   - The courts can find it difficult to deal with highly complex technical issues in the context of litigation.
   - Liability law varies from State to State, particularly in terms of the ways in which negligence and nonnegligence are defined. This creates a climate of uncertainty with respect to how the law will be applied.
2. *Insurance:* While secondary to liability law in importance, insurance is another method of controlling risk by spreading it over a large number of persons or organizations. Its cost is an incentive to the client to reduce risk. This is particularly true where there is a potential for catastrophic loss. In such cases, insurance companies generally require an extremely large deductible and/or impose limited liability ceilings. However, any attempt to turn to insurance as a mechanism to control risk must deal with the following Problems:

[6]David Okrent, "Comment on Societal Risk," *Science*, vol. 208, Apr. 25, 1980, pp. 372-395.

- insurance can be discriminatory in ways not deemed to be in the social interest;
- by concentrating on minimizing loss to the insured, broader social losses are ignored or underrated; and
- when the cost of the insurance is not a sufficient deterrent, it can actually encourage persons or organizations to assume risks that are not prudent.