Pergamon

Technology In Society, Vol. 12, No. 4, pp. 511–523, 1996

0160-791X/96 $15.00+0.00

S0160-791X(96)00029-2

Technological Vulnerability

Brian Martin

ABSTRACT. Technological vulnerability refers to the chance that a technological system may fail due to outside impacts. The usual approaches to studying technological risk are not so useful for studying vulnerabilities of major systems such as energy, communication, or defense. Analyzing the relation of interest groups to vulnerabilities can be illuminating. In some cases groups have interests in maintaining practices that cause vulnerabilities, while in other cases groups have interests in maintaining vulnerabilities themselves. These latter cases are especially difficult to deal with since they challenge prevailing belief systems.

Introduction

Every new technology seems to bring with it some new vulnerability for its users, a vulnerability to accident, disease, environmental degradation, or social disruption. With the automobile came traffic accidents. With electric appliances came exposure to electromagnetic fields. With the burning of fossil fuels came the greenhouse effect. With nuclear weapons came the possibility of megadeath.

The usual approach to these issues is through the concept of risk, which deals with the chance that specified adverse effects may occur due to operation or breakdown of the technology.[1] Risk is a useful concept especially when events are well specified and can be quantified, as in the cases of the collapse of a bridge or loss of power in an electricity grid. But for other purposes, the concept of vulnerability can be more illuminating.

To take an example, industrialized societies are becoming ever more

Dr Brian Martin is the author of numerous books and articles on scientific controversies, politics of technology, nonviolent defense, information and society, suppression of dissent, and other topics. His most recent books are Social Defence, Social Change *(1993) and* Confronting the Experts *(editor, 1996). He is senior lecturer in the Department of Science and Technology Studies, University of Wollongong.*

dependent on computers and hence highly vulnerable to disruption of computer-based services. Intentional sabotaging of vital computer programs in telephone systems, banks or factories could bring much commerce to a halt. More dramatically, a nuclear explosion high in the atmosphere would produce a continent-wide pulse of electromagnetic energy that could disrupt all sorts of microcircuits temporarily or even permanently.[2] New infectious diseases could arise and spread rapidly due to urbanization, poverty, new patterns of sexual activity and other changes creating an ecology favorable to certain microbes.[3] These sorts of contingencies, in which the possible consequences are enormous but the chance of an occurrence is difficult to determine because the cause is due primarily to social processes outside the system under threat, are usefully approached using the idea of vulnerability.

In the next section, I give a more precise definition of technological vulnerability. Then I turn to frameworks for classifying technological vulnerabilities, presenting a framework that distinguishes between vulnerable systems according to whether there are groups with an interest in perpetuating the vulnerabilities themselves. The focus is on large-scale vulnerabilities to which there has been relatively little attention.[4]

The Nature of Technological Vulnerability

To define technological vulnerability it is helpful to draw on systems theory and distinguish between a technological system and its environment.[5] The technological system might be, for example, a clothing factory or water supply system. The system includes artefacts (e.g., cloth and sewing machines; dams and pipes), relevant humans (factory workers; civil engineers) and associated skills and routines.[6] The "environment" is everything outside the technological system, and can include things like financial markets and earthquakes.

To achieve its intended purposes, a technological system requires certain inputs (raw materials, replacement workers, education, etc.) and produces certain outputs (finished clothing; water for consumers). The system's vulnerability can be defined as the chance that a specified change in the environment leads to disruption of the usual purposes of the system. For example, the threat to the clothing factory might be competition from imports, a strike by workers or a flood. The threat to the water supply system might be sabotage or a drought.

A technological system can be said to be resilient in the face of a particular threat if it is capable of maintaining its purposes when the threat is realized.[7] For example, the clothing factory will be more resilient in the face of a strike if there are other workers available with the skills required to keep production going. The water supply system will be more resilient against destruction of a dam if no single dam provides a large percentage of water for the system.

To quantify vulnerability and resilience, it would be necessary to provide

much more detailed specifications of various components in these definitions, including the distinction between the technological system and its environment, the nature of the threat and what is meant by the system "maintaining its purposes." Such precision is not necessary for the purpose here, which is to highlight significant features of technological vulnerability.

With the above definition, the distinction between technological risk and vulnerability becomes clearer. Technological risk usually refers to the danger to the public from technological systems, whether due to breakdowns or normal operations.[8] Examples are aircraft crashes and emissions from microwave ovens. Technological vulnerability, by contrast, refers to the chance of failure of an entire technological system due to outside events. Nevertheless, there is a close connection between the concepts of risk and vulnerability. Among other things, a system collapse resulting from exploitation of a vulnerability typically leads to the sorts of consequences analyzed in studies of risks.

Classification of Technological Vulnerabilities

There are quite a few ways to classify vulnerabilities, each of which is useful for some purposes but limited for others. Here I give a brief overview of a number of common frameworks before introducing yet another one. It is commonplace to discuss risks and vulnerabilities according to the type of technology involved. For example, chemical plants are vulnerable to malfunction as in the cases of Seveso and Bhopal. Nuclear power plants are subject to core meltdowns, terrorist attack and military attack, among other things. In recent years there has been considerable attention to vulnerabilities of computer systems.[9] Focussing on a type of technology has the obvious advantage of grouping systems with certain similar features. The complexities of large computer programs mean that certain types of failures are common wherever such programs are used.[10] On the other hand, focusing on a type of technology artificially divides common areas, such as energy systems including hydro, fossil fuel and nuclear components, where different types of technology combine to serve a single purpose.

Another approach is to divide vulnerabilities according to scale, namely the "size" of the disaster that might occur. When a software glitch in a radiotherapy machine causes a lethal overdose of radiation to a patient, a single person or at most a sequence of patients is affected. In an aircraft crash, a large number of passengers and crew can die. Then there are global processes such as reduction in stratospheric ozone due to emissions of chlorofluorocarbons and other chemicals, leading to an increase in skin cancer in many parts of the world, among other effects. In some cases, the scale of a vulnerability is not clear-cut. Automobile accidents seldom kill more than a few people at a time, yet in total such accidents leave many tens of thousands of people dead each year, which can be attributed to the technological system of car-based travel. The scale of consequences is an obvious

way to classify vulnerabilities but it is not so clear what insights this provides.

Another framework commonly used refers to the type of problem involved in causing a technological breakdown, such as human error, mechanical failure, shortcoming in system design or excessive complexity.[11] This sort of analysis can be very useful in focussing on areas where changes can be made to reduce the risks of a breakdown.

These different frameworks each have their advantages when dealing with technological risk, but they are of limited value for elucidating technological vulnerability. As noted above, vulnerability is defined in relation to a particular threat. In the classification schemes based on type of technology, scale or type of problem, the threat varies from case to case. Indeed, classifying vulnerabilities by type of problem is really, in a sense, classifying them according to different threats. None of these classification schemes really says much about the nature of system breakdown, especially when the system is large scale such as the food system or health system.

Because vulnerabilities are defined in relation to particular threats, it might seem that the only way forward is to look at particular cases. For example, in looking at the vulnerability of the entire system of road transport against breakdown, one might investigate threats due to a blockade of oil imports, terrorist attacks on petroleum refineries, or global economic collapse. In each of these examples, the basic problem is a shortage of reasonably priced fuel for vehicles.

A general method of analyzing technological vulnerabilities is as follows. First, write down every conceivable threat to the operation of the system in question. For each threat, write down the possible consequences. Next, write down possible responses to prevent or reduce the effect of each of the consequences. An example would be to look at the vulnerability of a country's computer networks to attack. Threats would include widespread sabotage, military takeover, and nuclear electromagnetic pulse. Consequences would include disabling of software, central political control, and physical destruction. Responses would include tighter security, unbreakable encryption and shielding against EMP. A much more detailed analysis has been made of the vulnerability of steel production to military threats.[12]

Since an analysis of vulnerabilities requires looking at specific threats, making generalizations would seem to be difficult. There are various ways around this obstacle. The approach adopted here is to look at interest groups and vulnerabilities to see whether there are interests in maintaining the vulnerabilities. This allows generalizations since the key question is whether there is a feedback loop between the vulnerability and its cause.

Interests and Vulnerability

The concept of "interest" is used to indicate that an individual or group has something to gain from a course of action, policy or practice.[13] For example, a scientist has an interest in being an author of a paper reporting a discovery;

a pharmaceutical company has an interest in a patented drug; a government has an interest in the perceived legitimacy of taxation. When interests are institutionalized through law or custom, they are commonly referred to as vested interests.

My concern here is with vulnerabilities that are perpetuated because of strong interests not just in practices causing the vulnerabilities but in the existence of vulnerabilities themselves. Some examples will help explain this phenomenon.

Consider the impact of chlorofluorocarbons on stratospheric ozone, setting aside other human processes that affect ozone.[14] Companies that produce aerosol sprays, refrigerants and the like have an interest in continuing production, sales and profits from these chemicals, but they certainly have no interest in the vulnerability of stratospheric ozone to chemical depletion. If this vulnerability did not exist, their corporate existence would be much more secure. The vulnerability of ozone to chlorofluorocarbons then is a case where there are no obvious interests in the vulnerability itself, though clearly there are corporate interests in activities that cause a hazard, "exploiting" the vulnerability.

Of course there might be some groups with an interest in the existence of this vulnerability of stratospheric ozone. Perhaps some environmental groups might be upset if the chlorofluorocarbon-ozone link were disproved, though it seems more likely that they would simply move on to other issues. Perhaps some manufacturers of sun-screens have an interest in worries about ozone depletion, which they can use to promote their products, though presumably other advertising angles could easily be found. The upshot is that it may be possible to unearth some individuals or groups with an interest in this particular vulnerability, but that the main relevant group—the chlorofluorocarbon industry—has no interest in it.

Most examples are like this: there are interests whose activities cause hazards, but these interests do not benefit from the existence of the hazard. In other words, there are no institutionalized interests in vulnerability itself. Producers and users of fossil fuels have an interest in practices that contribute to the greenhouse effect, but they have no obvious interest in the vulnerability of the earth's climate to human inputs of carbon dioxide and other chemicals. Manufacturers of motor vehicles have an interest in continuing use of these vehicles that happens to lead to tens of thousands of deaths on the road each year, yet these manufacturers have no interest in the vulnerability of road transport to accidents. Indeed, they have made considerable investments in methods of reducing accidents and their consequences, though not as many efforts as critics would like.[15] The same sort of analysis applies to innumerable risks and vulnerabilities more local in scale. Producers of microwave ovens have an interest in maintaining sales of a technology that poses a certain risk to health, but have no interest in the vulnerability of the human body to exposure to microwave radiation.

There are, though, a few cases in which it can be argued that there are strong interests in maintaining certain types of vulnerabilities. These cases

are inherently contentious, since few groups ever admit—to themselves or anyone else—that they foster vulnerabilities, especially when their rationale is to overcome these very vulnerabilities. Let me start then with an example—terrorism—that conforms to common viewpoints before turning to more significant ones that challenge conventional wisdom.

Terrorism can be defined as the use of threats or attacks on a population to cause fear and obtain compliance with demands. Non-state terrorists[16] often exploit technological vulnerabilities, such as the vulnerability of an aircraft, passengers and crew to a bomb or a few armed individuals. These terrorists have an interest in maintaining this vulnerability. But they have little say in the perpetuation of the vulnerability, since they do not control aircraft manufacture, choice of transport mode, etc. Thus while terrorists have an interest in technological vulnerability, they have little control over the existence of the vulnerability itself.

For a more comprehensive and challenging example, consider the system of liquid-fuel-based road transport, including cars, trucks, roads, oil companies, automobile manufacturers, and government transport departments, among others. This technological system is highly vulnerable to a shortage or cut-off of oil, which might be caused by sabotage of petroleum refineries, strikes by oil company workers, a blockade of oil imports or war in oil-producing regions.[17]

There are various ways to reduce this vulnerability or, in other words, to increase the resilience of the transport system in the face of a cut-off of oil supplies. Possibilities include stockpiling fuel, developing diversified sources of supply, preparing rationing systems, and promoting fuel efficiency. These provide some cushion against emergencies but do not remove the underlying vulnerability.

Another approach is to move towards a transport system that relies far less on liquid fuel. This could include dramatically improved public transport, telecommuting, and redesign of cities so that most trips can conveniently be made by walking or cycling. Such an alternative has often been advocated and a number of cities have made moves in this direction,[18] but the vulnerability remains a significant one. Why?

The interests behind a transport system based on oil are enormous: oil companies, car manufacturers, road-building industries and government roads departments, among many others. This is one of the most powerful industrial-bureaucratic complexes in the world.[19] Parts of this complex have an interest in selling oil products, selling cars, building roads, and so forth. Can it also be said that they have an interest in the vulnerability of a transport system to shortages of liquid fuel?

The case for this is especially strong in the United States, which has massive oil reserves of its own. Nevertheless, U.S. production is not enough to serve the country's huge consumption of cheap oil and there is massive importation of oil, especially from Gulf states. Even very moderate conservation measures, such as switching to smaller and more efficient vehicles like those commonly in use in Europe and Japan, would eliminate the need

for oil imports to the United States, eliminating its dependence and hence one vulnerability. But this path has not been adopted. Instead, national policy has centered on maintaining access to cheap overseas oil. This has meant putting pressure on foreign governments, occasionally conspiring to overthrow them and going to war.[20] A very risky and interventionist foreign policy has been adopted which would be quite unnecessary if some simple conservation measures were adopted.[21]

There are various ways to understand this promotion of energy vulnerability. One is to argue that U.S.-based oil companies seek to maximise their share of the world market by controlling foreign oil fields, and have directly or indirectly shaped the U.S. policy-making agenda to serve their interests in this respect.[22] It is also possible to delve more deeply and to argue that both corporations and states prefer energy options that make consumers dependent on their services. Reserves of liquid fuels are very unevenly distributed over the globe and this means that small groups can easily take control over them; they have an interest in making others dependent on these fuels. By contrast, solar energy is relatively evenly distributed and much harder to monopolize, hence the much lower interest by corporations.[23] A similar set of arguments applies to governments. Raising revenue is much more straightforward when the population is dependent for survival on commodities that are controlled by government or large corporations.[24] The liquid-fuel-based transport system is ideal for collecting taxes on fuel, vehicles, etc. The prospects for taxation on travel when town planning allows people to walk to work are much less.

A little reflection reveals that these arguments apply to centralized energy sources of all kinds. For example, in the production of electricity, large hydroelectric plants, nuclear power, and large fossil-fuel plants are all vulnerable to terrorism, sabotage and military attack in a way that microhydro, passive solar design and local solar and wind electricity systems are not. Arguably, there is more involved here than simply efficiency considerations. In early 1950s, the U.S. Paley Commission recommended increased use of solar energy, but instead major investments were poured into nuclear power.[25] This sort of choice can be analyzed at several levels. For organizations administering technological systems for large populations—energy or water boards, for example—it is "easier" to deploy experts, raise funds and mobilize political support for large-scale projects than to foster a process of small-scale change. A new dam is built rather than fix leaky faucets throughout the city; a new power plant is built rather than install energy-efficient heaters and air conditioners.[26] To say that building new centralized capacity is an "easier" option hides a key factor: this approach makes necessary the central administering organization itself. Associated with this, it requires the attention of experts, including financial managers, engineers, and police (the latter to protect against attacks on vulnerable systems). More generally, centralized energy production is congruent with the centralized administrative apparatuses associated with the state.[27]

I have devoted considerable attention to features of centralized energy

systems, presenting the argument that certain groups have an interest in vulnerabilities of these systems, namely those vulnerabilities that are linked to the population's dependence on centralized provision of energy. Much more could be said about this issue without necessarily resolving it. My point is that there is a case that some powerful groups may have an interest in maintaining technological vulnerabilities. The following examples are outlined even more briefly.

Among the salient vulnerabilities of every society today is vulnerability to military attack. This includes attacks by a country's own military on indigenous populations, civil war, invasion, and the consequences of global nuclear war. Many of these threats are created or perpetuated at least in part by the very institutions designed to oppose them. The most familiar is nuclear deterrence: nuclear weapons pose a threat to other countries, justifying acquisition of nuclear forces by other governments, thereby justifying the need for nuclear weapons in the first place. But the phenomenon of military races applies much more widely, of course.

Looking more deeply, the very possession of armed forces has been described as a "protection racket."[28] The military must be funded, typically requiring a sizable slice of the government budget. Those who refuse to pay their taxes are compelled to by the police power of the state, ultimately backed up by the military. In many countries, militaries are irrelevant or inadequate for defense against outside attack. Their main purpose is to prop up the ruling regime, sometimes with murderous consequences.

This view of the military is of course completely at variance with the usual idea of "defense." Interest groups linked to the military naturally foster a belief system—in which they themselves believe implicitly—that sees military forces as essential to protect against both enemy troops and internal subversives. It is well known that militaries are prone to exaggerate the threat from potential enemies. From their point of view it is best to be prepared for the worst contingencies; others perceive a self-serving element. Whatever the motivation, militaries by their existence serve to create vulnerabilities to military attack.

Military-induced vulnerabilities are increasingly technological. Vast investments are made in research, development and production of ever more sophisticated weapons systems.[29] Many of these weapons, especially the potentially offensive ones such as bombers and missiles, create greater vulnerability, since the ability to attack is seen as a deterrent.[30] The nuclear arms race is the ultimate in self-justifying technological vulnerability.

Alternatives to militaries have received little attention, certainly far less than alternatives to centralized energy supplies. One possibility is nonviolent defense based on civilian action using techniques such as strikes, boycotts, sit-ins and noncooperation.[31] The case for such an alternative cannot be canvassed here; suffice it to say that on the basis of many studies and actual uses of nonviolent action it seems worthy of attention but has received very little, least of all in terms of developing technology for nonviolent struggle.

One plausible reason for this is the strong interests behind maintaining military systems and their associated vulnerabilities.

Another example where there seem to be significant interests in maintaining vulnerabilities involves the complex issue of cash crops in the Third World. When farmers grow food that they can eat themselves or sell locally, this provides communities some degree of resilience against the vagaries of international markets. To increase export income, many Third World governments have promoted production of crops for export, such as coffee, tea or bananas. This can increase incomes, at least of some farmers, but at the expense of increased vulnerabilities. A political factor becomes prominent here. Many Third World countries are run by repressive rulers, either military dictatorships or figurehead democracies. These regimes are maintained by force, not least against any challenge to prevailing economic inequalities. It is easier to maintain repressive rule when the population is not self-reliant.[32] Producing cash crops makes it harder for popular opposition movements to build support. This process is fostered by the so-called structural adjustment programs commonly imposed by the World Bank and International Monetary Fund as a condition for providing finance. Technology enters this complex process through the dependence of cash crops on pesticides, artificial fertilizers and genetically engineered seeds.

The Third World agriculture package fosters vulnerability of farmers to both repression and interruption of technological inputs through the interlinked interests of international financial systems and repressive rulers. Without exports of cash crops, rulers cannot pay for imports of goods from the first world, including military and police technology used to maintain their rule.

Illegal drugs provide another case where it can be argued that there are interests in maintaining vulnerabilities. The issue of whether specific drugs should be legal or illegal—with various shades of grey in terms of types and degrees of regulation—is highly contentious on its own, not to mention the argument here that certain groups have interests in maintaining vulnerability to drug-related hazards. Nevertheless, let me present the argument. A number of researchers have argued that society would be better off if certain drugs, now illegal, were decriminalized or legalized.[33] The paradigm case is marijuana.[34] A complex of interests maintains the current legal regime, including politicians who campaign on drug scares and some enforcement agencies. More diffuse is the interest of a broad cross-section of the population in the stigmatizing of users of currently illegal drugs. Because of highly selective enforcement of drug laws, it is primarily the poor, unemployed and minority groups that are arrested and jailed for drug use or sales. The enormous and continually growing prison population in the United States is partly attributable to a prison-industrial complex that owes much to drug policies.[35]

Many of the health hazards of illegal drugs are due to their illegality. Legal drugs are obtainable in reliable and unadulterated doses; quality control of illegal drugs is difficult. Many middle-class doctors maintain opioid habits

for years with no physical or legal problems; street users are likely to suffer overdoses and arrests. Crime associated with illegal drugs is aggravated by enforcement policies: police seizures of drugs drive up prices, leading to greater involvement by criminals willing to take greater risks.

To be sure, there is a counterargument to be made about the greater hazards from legalization of currently illegal drugs. The point here is that it can be argued that certain drug-related vulnerabilities—the vulnerability of individual drug users to impure drugs and to arrest and the vulnerability of society to drug-related criminal activity—persist because it is in the interest of certain groups to maintain these vulnerabilities.

As mentioned at the outset, it is difficult to provide convincing examples of vulnerabilities that are perpetuated by vested interests, because of entrenched belief systems that these very interests are necessary to protect against the vulnerabilities. Centralized energy sources seem to be required to provide the reliability in energy supplies that people have come to expect; military forces seem to be required to protect against military attack; cash cropping seems to be necessary to provide income for survival and prosperity; laws against drugs seem to be necessary to prevent even greater hazards from uncontrolled drug use. At one level, these beliefs are correct. The vulnerabilities associated with these systems have grown along with the systems themselves and cannot be banished by any quick fix. It is tempting to call these vulnerabilities "self-reproducing" in that sociotechnical systems help create the demand for their own existence. Since this terminology might suggest that this process is autonomous, perhaps a better description is the clumsy "interest-reproducing vulnerabilities."

Conclusion

There is far more attention given to technological risk, namely the consequences of the failure of technological systems, especially hazards to the public, than to technological vulnerability, which focuses more on how a technological system may fail due to outside impacts. The most interesting, important, and challenging vulnerabilities are ones associated with large-scale systems such as energy, agriculture, and economics. How should such vulnerabilities be studied? Typical approaches divide risks and vulnerabilities according to the type of technology, the scale of the hazard or the modes of failure. Each of these approaches has advantages, but none provides much insight into the persistence of significant vulnerabilities of large-scale systems.

Analysis of interests provides a useful method of analysis. In a first category of cases, no major group is linked to the vulnerability. In such cases, a rational examination of the issues and responses faces fewest obstacles, though action may be stymied by disputes over what, if any, preventive measures should be taken and who will pay for them.

In a second category of cases, vulnerabilities are associated with the activities of powerful interests but the dangers do not serve these interests. In

such cases, such as factory hazards and the greenhouse effect, agreement on the value of reducing the vulnerability is relatively easy; disagreement occurs over the trade-off between the costs and benefits of hazard reduction, whether this is installation of safety equipment in factories or reducing use of fossil fuels. The path for hazard reduction is clear: the debate is over how far down it to travel.

In a third category of cases it can be argued that powerful groups have an interest not just in maintaining practices that lead to a danger but in maintaining vulnerability itself. For example, militaries justify their existence by the need to protect against threats that are partly provoked by their existence in the first place. This sort of analysis is inherently contentious since no interest group is likely to welcome a conclusion that it is responsible for maintaining a vulnerability that it is supposedly there to overcome or limit.

Analyzing the role of interests in vulnerabilities carries with it the implicit suggestion that overcoming these vulnerabilities requires a challenge to the interests; rational persuasion is unlikely to be successful on its own. Even when there is no interest in a vulnerability, the interests involved can be incredibly powerful, as in the case of fossil fuel producers and users in the case of the greenhouse effect. Yet there is an extra dimension to the task facing those who wish to tackle vulnerabilities in which interests have a stake, such as military vulnerabilities. This extra dimension is the deep-seated beliefs in systems that create the need for their services.[36] This extra dimension also makes the task in this paper of presenting a case that such vulnerabilities exist a challenging one.

Acknowledgment

Stewart Russell provided helpful comments.

Notes

1. See, for example, S. L. Cutter, *Living with Risk: The Geography of Technological Hazards* (London: Edward Arnold, 1993); Theodore S. Glickman and Michael Gough (eds.), *Readings in Risk* (Washington, DC: Resources for the Future, 1990); W. W. Lowrance, *Of Acceptable Risk: Science and the Determination of Safety* (Los Altos, CA: William Kaufmann, 1976).
2. M. Wik, "URSI Factual Statement on Nuclear Electromagnetic Pulse (EMP) and Associated Effects", *International Union of Radio Science Information Bulletin*, Vol. 232 (1985), pp. 4–12
3. L. Garrett, *The Coming Plague: Newly Emerging Diseases in a World Out of Balance* (New York: Farrar, Straus and Giroux, 1994). It is conceivable that new diseases may arise due to medical procedures. See, for example, B. F. Elswood and R. B. Stricker, "Polio Vaccines and the Origin of AIDS," *Medical Hypotheses*, Vol. 42 (1994), pp. 347–354.
4. C. Kearton, and B. Martin, "Technological Vulnerability: A Neglected Area in Policy-Making", *Prometheus*, Vol. 7 (1989), pp. 49–60
5. F. E. Emery (ed.), *Systems Thinking* (Harmondsworth: Penguin, 1981).
6. I take it as a given that "technology" includes both technical and social aspects. A "technological system" could also be called a "sociotechnical ensemble."
7. Depending on the threat, flexible systems—see D. Collingridge, *The Social Control of Technology* (London: Frances Pinter, 1980)—are more likely to be resilient.
8. Accidents can be considered to be a normal part of the operation of any system, as argued by C. Perrow, *Normal Accidents* (New York: Basic Books, 1984).

9. Jacques Berleur, Colin Beardon and Romain Laufer (eds.), *Facing the Challenge of Risk and Vulnerability in an Information Society* (Amsterdam: North-Holland, 1993); P. G. Neumann, *Computer-Related Risks* (New York: ACM Press, 1995).
10. B. Littlewood and L. Stringini, "The Risks of Software", *Scientific American*, Vol. 267 (1992), pp. 38-43
11. See Perrow, *op. cit.*
12. C. Kearton and B. Martin, "The Vulnerability of Steel Production to Military Threats", *Materials and Society*, Vol. 14, no. 1 (1990), pp. 11-44
13. See, for example, B. Barnes, *Interests and the Growth of Knowledge* (London: Routledge and Kegan Paul, 1977).
14. A nice treatment of the interaction of interests and knowledge in the ozone debate is given by L. Dotto and H. Schiff, *The Ozone War* (Garden City, NY: Doubleday, 1978).
15. See, for example, A. Irwin, *Risk and the Control of Technology: Public Policies for Road Safety in Britain and the United States* (Manchester: Manchester University Press, 1985).
16. Contrary to popular opinion, most terrorism is carried out or sponsored by major governments, not the small groups or renegade regimes that are the focus of most attention. See E. S. Herman, *The **Real** Terror Network: Terrorism in Fact and Fiction* (Boston: South End Press, 1982).
17. W. Carsnaes, *Energy Vulnerability and National Security: The Energy Crises, Domestic Policy Responses and the Logic of Swedish Neutrality* (London: Pinter, 1988); W. Clark and J. Page, *Energy, Vulnerability, and War: Alternatives for America* (New York: Norton, 1981); A. B. Lovins and L. H. Lovins, *Brittle Power: Energy Strategy for National Security* (Boston: Brick House, 1982); James L. Plummer (ed.), *Energy Vulnerability* (Cambridge, MA: Ballinger, 1982).
18. T. Bendixson, *Instead of Cars* (London: Maurice Temple Smith, 1974); C. Ward, *Freedom to Go: After the Motor Age* (London: Freedom Press, 1991).
19. J. J. Flink, *The Car Culture* (Cambridge, MA: MIT Press, 1975); D. A. Taebel and J. V. Cornehls, *The Political Economy of Urban Transportation* (Port Washington, NY: Kennikat Press, 1977).
20. The most well known examples are the CIA-assisted overthrow of the Iranian government in 1953 and the 1991 Gulf war.
21. This argument has been made best by Lovins and Lovins, *op. cit.* See also A. B. Lovins, *Soft Energy Paths: Toward a Durable Peace* (Harmondsworth: Penguin, 1977).
22. It may not be necessary for powerful groups to make active efforts in order for others to serve their interests. See M. A. Crenson, *The Un-Politics of Air Pollution: A Study of Nondecisionmaking in the Cities* (Baltimore: Johns Hopkins University Press, 1971).
23. G. Boyle, *Living on the Sun: Harnessing Renewable Energy for an Equitable Society* (London: Calder and Boyars, 1975), pp. 14, 16, 58.
24. On the link between the rise and survival of the state and the power to extract resources from the economy, see for example H. Jacoby, *The Bureaucratization of the World* (Berkeley: University of California Press, 1973); M. Levi, *Of Rule and Revenue* (Berkeley: University of California Press, 1988).
25. R. Nader and J. Abbotts, *The Menace of Atomic Energy* (Collingwood, Victoria: Outback Press, 1977), pp. 29-31.
26. M. Lönnroth, P. Steen and T. B. Johansson, *Energy in Transition: A Report on Energy Policy and Future Options* (Uddevalla, Sweden: Secretariat for Future Studies, 1977), pp. 13-14, make this point in relation to Swedish energy policy in the 1950s, namely that from the point of view of central administration it is more complicated to administer a policy of energy conservation than one of increasing energy supply.
27. See, for example, A. Gorz, *Ecology as Politics* (Boston: South End Press, 1980); Robert Jungk, *The New Tyranny: How Nuclear Power Enslaves Us* (New York: Grosset and Dunlap, 1979); L. Solomon, *Energy Shock: After the Oil Runs Out* (Toronto: Doubleday, 1980).
28. C. Tilly, "War Making and State Making as Organized Crime," in Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol (eds.), *Bringing the State Back In* (Cambridge: Cambridge University Press, 1985), pp. 169-191. See also E. Krippendorff, *Staat und Krieg: Die Historische Logik Politischer Unvernunft* (Frankfurt: Suhrkamp, 1985), as reviewed by J. Galtung, "The State, the Military and War," *Journal of Peace Research*, Vol. 26 (1989), pp. 101-105; B. D. Porter, *War and the Rise of the State: The Military Foundations of Modern Politics* (New York: Free Press, 1994); C. Tilly, *Coercion, Capital, and European States, AD 990-1992* (Cambridge MA: Blackwell, 1992).
29. See, for example, Everett H. Mendelsohn, Merritt Roe Smith and Peter Weingart (eds.), *Science, Technology and the Military* (Dordrecht: Kluwer, 1988).
30. An exception to this is so-called "non-offensive defense" which relies on weapons that are not easy

to use for attack, such as short-range fighter aircraft. Only a few governments have seriously investigated this sort of defense system.

31. See, for example, A. Boserup and A. Mack, *War Without Weapons: Non-violence in National Defence* (London: Frances Pinter, 1974); M. Randle, *Civil Resistance* (London: Fontana, 1994); Adam Roberts (ed.), *The Strategy of Civilian Defence: Non-violent Resistance to Aggression* (London: Faber and Faber, 1967); G. Sharp with the assistance of B. Jenkins, *Civilian-Based Defense: A Post-Military Weapons System* (Princeton: Princeton University Press, 1990).
32. D. V. Porpora, *How Holocausts Happen: The United States in Central America* (Philadelphia: Temple University Press, 1990), Chapter 4, points out how the social structures of dependence and inequality—including cash cropping—lead to mass hunger. On the state as a hazard, specifically the link between government repression, technological vulnerability and famine in the Third World, see B. Wisner, "Disaster Vulnerability: Scale, Power and Daily Life," *GeoJournal*, Vol. 30 (1993), pp. 127-140.
33. J. B. Bakalar and L. Grinspoon, *Drug Control in a Free Society* (Cambridge: Cambridge University Press, 1984); S. B. Duke and A. C. Gross, *America's Longest War: Rethinking Our Tragic Crusade against Drugs* (New York: G. P. Putnam's Sons, 1993).
34. L. Grinspoon, *Marijuana Reconsidered* (Cambridge, MA: Harvard University Press, 1971).
35. N. Christie, *Crime Control as Industry: Towards Gulags, Western Style* (London: Routledge, 1994, second edition).
36. This is a theme running through the incisive critiques of education, energy, health and other systems by Ivan Illich. See *Deschooling Society* (London: Calder and Boyars, 1971); *Energy and Equity* (London: Calder and Boyars, 1974); *Medical Nemesis: The Appropriation of Health* (London: Calder and Boyars, 1975); *The Right to Useful Unemployment and its Professional Enemies* (London: Marion Boyars, 1978).