TECHNOLOGICAL VULNERABILITY: A NEGLECTED AREA IN POLICY-MAKING*

Colin Kearton and Brian Martin

Many technological systems are vulnerable to threats such as military attack, sabotage, sudden economic change or social disaffection. There are various ways to reduce such vulnerabilities, such as direct planning, diversification and self-reliance, but current policy-making takes little cognisance of the issue.

Keywords: vulnerability, resilience, risk, policy-making

Australia's highly sophisticated telecommunications network is an open target for saboteurs. When someone chopped through a set of Telecom cables in 1987, it interrupted a large proportion of Sydney's telephone service.

A small number of workers at one of Australia's larger oil refineries, by deciding to go on strike, can threaten the entire economy by interrupting the vital flow of liquid fuel. Much of Australia's petroleum production in the Bass Strait is an open target for small commando or terrorist groups. Again, the entire economy could be affected.

The $160 million Australian Animal Health Laboratory was opened in 1984 in Geelong. Designed at great expense to handle live foot-and-mouth disease virus, the organised opposition of farmers has meant that the laboratory is not being used for its intended purpose.[1]

These are examples of vulnerabilities in contemporary Australian society which are associated with technologies — 'technological vulnerabilities' for short. They are vulnerabilities of crucial systems to a variety of serious but very unlikely threats coming from outside the technological systems themselves.

When technological systems are set up, due attention is usually given to the obvious and routine threats. A factory building will be constructed according to specifications to ensure it is not faulty, routine security measures will be taken to prevent vandalism, and an assessment of markets will be made before producing a new product. By contrast, some other threats are ignored entirely, typically threats which are considered

* This work was supported by the Australian Research Grants Scheme. We thank the many employees of BHP Steel at Port Kembla who we interviewed for their cooperation and their valuable comments, and Michael McKinley, Stewart Russell, Pam Scott and an anonymous referee for useful comments on a first draft of this paper.

by planners to be unlikely, impossible or too expensive to guard against. The factory building will not be constructed, in Australia at least, to survive a major earthquake or a military attack; nor will market planning for export seriously take into account the possibility of world economic collapse. It is vulnerabilities to such unlikely but serious contingencies that are the focus of our attention here.

What we call technological vulnerability can be distinguished from the related and partially overlapping category of technological risk. In the latter category fall events such as the Chernobyl nuclear power plant meltdown, the Bhopal chemical plant disaster, the Challenger space shuttle failure and the shooting down of the Iranian Airbus. In these accidents the dominant focus is on technological failures most of which are the immediate consequence of internal breakdowns (though having wider social roots) and most of which result in hazards to the public. Some of the literature on risk assessment deals with the processes involved in such events.[2] Attention is usually given to failures in individual units of a wider system, such as accidents in particular power plants rather than the failure of the entire electricity grid.

By contrast with this category of technological risk, our focus on vulnerability is on the major technological systems themselves and the ways in which they may fail or become obsolete due to events in society largely external to the technological system. In short, in technological risk the focus is on hazards to the public from localised technological failures while in technological vulnerability the focus is on failure of extensive technological systems due to outside impacts. Where the study of technological risk may connect with technological vulnerability is in offering certain tools for analysis, such as judging a risk by its probability times its severity.

The study of what we call technological vulnerability has been sparse, unsystematic and driven by events. The area of greatest interest has been energy, triggered by the threats to exports of Middle East oil from 1973 onwards.[3] This has led to examination in oil-importing countries of a variety of strategies, including stockpiling, rationing, indigenous oil production, alternative sources of imports, energy efficiency, and developing non-petroleum energy sources including coal, nuclear and solar power.

Another area of interest has been computers, especially in their role in the systems used to launch a nuclear weapons attack or guard against such an attack. A straight military concern is the vulnerability of command, control and communications systems to enemy action; wider concerns have been expressed about the danger of accidental nuclear war.[4]

Although there is some useful material in specific areas such as energy and computers, the wider issue of technological vulnerability has received surprisingly little attention. In this paper we aim to give a brief overview of the issues. We begin by describing some threats and then describe how the vulnerabilities and resiliences of different technologies arise and

interact. We itemise a range of ways to reduce vulnerabilities, and finally suggest some policy implications.

It is not our aim here to argue that resilience to remote threats is an overriding goal in technological policy. It is simply one factor among many that should be taken into account in a careful consideration of options. But at the moment many aspects of vulnerability and resilience are given little attention at all. To change this could provide a bit of insurance, at low cost, against the possibility of catastrophe.

THREATS

The number and variety of possible threats to technological systems is large. Here we note a selection of different threats which illustrate a range of dangers and effects.

- Collapse of markets. A sudden change in overseas circumstances, such as a world economic depression, a trade war or revolutionary change, could lead to a dramatic reduction in export markets. The technological infrastructure developed to serve these markets would thus become obsolete.
- Loss of markets. New trends or inventions can lead to sudden loss of markets. The collapse of the Swiss mechanical watch-making industry in the face of digital watches is an example. Viable synthetic substitutes for wool or beef, into which research is continuing, would see those Australian industries go the way of natural rubber.
- Social disaffection. Massive investments made in certain technologies may be wasted if opposition makes it impossible to use them fully. The opposition to nuclear power in many countries has meant that some highly expensive plants have not been completed or, after completion, not been used. If the Australian government had persisted with its national identity card plan, it is possible that citizen non-cooperation would have wrecked the scheme and thus caused the investment in it to be wasted.

The above possibilities could, without causing physical damage, make technological systems obsolete or unworkable. The following threats could destroy or interrupt their functioning.

- Sabotage. Teams of saboteurs or terrorists, or even a few dedicated individuals, could wreak havoc in a range of technological systems.[5] Insiders pose the greatest threat; a single strategically placed individual could, in many industries, bring operations to a halt. The axing of Telecom cables is an example.
- Interruption of imports. A major nuclear war in the northern hemisphere could decimate industrial production in Europe, Japan and North America while leaving Australia physically unscathed.[6]

Most imports would cease, leading quickly or eventually to severe problems with many technologies: as breakdowns occurred, replacements or spare parts normally imported would be unavailable or highly expensive. Another scenario with a similar outcome would be a naval blockade of Australian ports.[7]

- Direct military attack. Some major facilities may be targeted because of their strategic or economic value, such as airports, seaports, communications bases, oil refineries, aluminium smelters, dams and power stations. Other facilities would suffer 'collateral damage' from attacks made for other purposes. A major attack, whether nuclear or conventional, on a metropolitan area would probably disable electricity and water distribution systems and most communications systems.
- Electromagnetic pulse. A nuclear weapon exploded high above the atmosphere leads to a pulse of electromagnetic radiation over an area as wide as a continent.[8] The voltage rise induced by the pulse can be ten times as great as for lightning. It is likely that all microcircuits not specially protected would be disrupted — affecting computers, electricity supplies and so forth — and it is possible that such circuits could be permanently damaged.

The likelihood of the above threats is obviously open to debate. While the view of most Australian military experts is that global nuclear war is extremely unlikely,[9] others disagree. For example, there seems to be a variety of assessments of the likelihood of accidental nuclear war.[10] The Swedish and Swiss governments have implemented extensive civil defence programmes on the basis of their continuing strategic evaluations, unlike most other countries. The New Zealand Planning Council has carried out an extensive assessment of how nuclear war would affect New Zealand, something which has never been done in Australia.[11] Not surprisingly, there are differences between countries and differences between different groups within any country as to whether certain threats necessitate advanced thought and planning. Our contention is that in many instances technological vulnerability has been neglected because there is no group which has any immediate interest in examining it.

VULNERABILITY AND RESILIENCE

A technological system can be defined as a patterned arrangement of artefacts and humans designed for a purpose. If the purpose is satisfied, the system is said to 'work'. Any sudden change in the external or internal environment — an earthquake, a strike or change in preference by users — poses a threat to the system. If the system is in danger of not working when a particular threat is realised, it is said to be vulnerable to that threat. If instead the system can continue to satisfy its purposes,

typically by rapid adaptation, it is said to be resilient in the face of that particular threat.

There are various reasons why a technological system becomes either vulnerable or resilient to a particular threat. First, there may be direct planning to handle certain contingencies. For example, to prevent social disaffection, promoters of a technology may engage in advertising, lobbying, attacking opponents or involving them in decision-making.

Second, the system may have been designed to survive a related threat, and this may provide resilience against the threat in question. For example, electricity supplies for continuous-process manufacturing must not be interrupted. For maintenance purposes, double or triple lines and junction boxes may be provided. This also provides resilience against vandals who strike out randomly at cables, even though vandals may not have been considered in the planning.

Third, the wider configuration of technological-social systems in the society greatly affects vulnerabilities. If all imports were cut off, the capacity of industries to continue production would depend on the capacity of *other* industries to provide raw materials, spare parts, skilled labour, etc.

Finally, chance often plays a role in providing resilience. It is essentially geological chance that put Australia's major oil fields in the Bass Strait where they are vulnerable to sabotage.

Of these four reasons for vulnerability or resilience, three are reasonably straightforward to analyse: direct planning, planning for related threats, and chance. The other reason, the organisation of technological, economic and social systems, is more complex and interesting. To illustrate the factors involved, we outline some of the interactions between vulnerabilities and resiliences in the three crucial areas of computers, electricity and steel manufacturing, focusing on one particular threat, interruption of imports.

Consider first the production of steel. Australia's steel is largely produced by integrated plants, which depend on a variety of imported materials, including some raw materials, refractories and electronic equipment. Without imports, steel production could only continue if local suppliers or substitutes could be found.

Electricity supplies from state electricity authorities are essential to steel production. Therefore, an analysis of the impact of cessation of imports on the electricity supply industry would be necessary to assess whether or how much steel production could continue.

Computers are becoming increasingly vital to steel production. Reverting to manual methods would be possible at the expense of increased use of labour, but as computerisation continues the difficulty of reversion becomes ever greater. Because computer chips are not manufactured on any scale in Australia, restriction of imports would be followed by gradual loss of computers, cannibalisation of some computers to keep others going, and eventually conversion to non-computerised methods — unless some local computer manufacturing

capability could be built up quickly. Therefore the resilience of the steel industry to interruption of imports depends on Australia's capacity to produce computing equipment.

Working in the other direction, the capacity to produce electricity in Australia without imports would depend on repairing and eventually replacing generating plants, maintaining coal production, or introducing new sources such as wind-powered generating plant. In all cases, the production of steel and other high quality metals would be essential. Thus, the resiliences of the steel and electricity sectors are mutually dependent.

The full picture would need to take into account further sectors, the strength and detailed implications of mutual interactions, the likely time delays involved as non-replaceable imported equipment gradually broke down, issues of skills and availability of labour, possibilities of doing with less steel, electricity and computer power, and other threats occurring at the same time.

While the total assessment of vulnerability and resilience is complex, it is possible with detailed analysis to separate crucial from marginal vulnerabilities and to focus on key areas of concern. In our study of vulnerabilities of the Australian steel industry to military threats, it quickly became apparent that certain imports, such as limestone and electrical equipment, could easily be obtained or produced locally, whereas others, such as iron ore (from Western Australia) and computers (from overseas), would be very hard to obtain should shipping to and around Australia be blockaded or otherwise interrupted.[12]

THE STEEL MINIMILL

The case of the steel minimill epitomises the neglect of issues of vulnerability and resilience in policy-making. This century, the standard method for steelmaking has been the integrated plant. This includes coke ovens for producing coke from coal, blast furnaces (using the coke) for producing iron from iron ore, basic oxygen furnaces (earlier, the open hearth) for producing steel from iron, and a multitude of rolling mills for producing rails, tubes, sheet and other forms from hot steel. The integrated plant requires a large investment, careful physical location for obtaining large quantities of inputs such as coal, iron ore, limestone and water, and a stable market for standard products. The scale of integrated plants is large, typically millions of tonnes of steel per year. In Australia, almost all steel production takes place at three integrated plants at Port Kembla, Newcastle and Whyalla.

In the past couple of decades, economic conditions have provided opportunities for a competing technology, the so-called minimill. The minimill typically uses an electric furnace to make steel directly from scrap, and then with a limited rolling operation fashions products such as rods, bars, wire and tubes. Because its main physical inputs are scrap

and electricity, and because its size is usually much smaller (with output perhaps one-tenth of an integrated plant), minimills can be built close to markets, often in the middle of cities. The smaller capital requirements mean that output is more readily adapted to changing market conditions.

In the United States and Europe, minimills have taken a rapidly growing proportion of steel production.[13] Technical advances in electric furnaces and in quality control in small milling operations have made them competitive in terms of material outputs; economic changes, especially a stagnant market for steel and hence lower prices for scrap, plus high interest rates and hence a premium on rapid construction, have made minimill operations economically competitive.

Another major factor, at least in the United States, is the cost of labour. Accommodation to strong trade unions has meant that labour costs in integrated plants are far higher than the average in manufacturing industry. Minimills have typically been located where they can rely on non-unionised labour at far lower wages.[14]

The Australian move towards minimills has been slower than overseas, perhaps because of the dominance of BHP and its heavy investment in integrated plants. Only one minimill has been built, by Smorgons in Melbourne.

BHP's plan to build a minimill in Rooty Hill (western Sydney) has met with a storm of opposition. Rooty Hill residents oppose it because of environmental considerations (and, no doubt, consequent reductions in property values). Wollongong trade unions and council officials say the minimill should be built in Wollongong — where Australia's largest integrated steel plant resides — because of the region's high unemployment rate. Many workers would also see the Rooty Hill location as offering BHP a way to escape the power of the trade unions in Wollongong.

Through this debate, the issue of vulnerability and resilience of steel production has not been raised.[15] A basic feature of the centralised and capital-intensive nature of integrated plants is that they are highly vulnerable to a variety of threats, including military attack, natural disaster and sabotage, not to mention rapid technological change. For example, one study of the effect of 'small' nuclear attacks on the United States showed how few bombs are necessary to destroy a large fraction of production in various areas of industry, of which steel is a crucial one.[16]

The rise of the minimill has made the steel industry much more resilient to such threats. The larger the number of independent plants there are, the less vulnerable is steel production to the failure of a specified few of them. For example, militarily it would be much easier to disable three integrated plants than 30 minimills. Furthermore, since minimills commonly only run two shifts, they would be able to greatly exapnd output in an emergency. In the type of crises envisaged, scrap would be plentiful due to possible destruction of the built environment, comprehensive recycling and lowered production which would extend

existing supplies of scrap. Furthermore, with a proliferation of minimills, there would be greater capacity to provide replacement parts and, if necessary, to cannibalise one plant to keep others going.

In Australia, with its high dependence on three integrated plants, the contribution of minimills to resilience in the face of exceptional but serious threats would be substantial. Yet no constituency has raised the issue of resilience. The federal government and the Defence Department do not enter this facet of technology and economic policy, since it appears to be largely an issue for private companies and local government planning. In the case of the proposed Rooty Hill plant, citizen groups and trade unions are more concerned about the immediate issues of environment and jobs than the apparently remote issue of vulnerability. The net result of this policy neglect is that the vulnerabilities and resiliences of the steel industry are largely unplanned consequences of decisions made for other reasons.

RESPONSES

There is a range of ways to increase the resilience of technological systems to major potential threats. Here we list and briefly comment on some of these ways before turning to their policy implications.

- Direct planning. This is the most obvious and one of the most neglected ways to increase resilience. For example, the serious possibility of nuclear attack as well as major attack using conventional weapons has existed for decades. Yet only a few governments have instituted more than token programmes of civil defence. Although the cost of such programmes is substantial, a society-wide cost-benefit analysis, even with an extremely low estimated risk of attack, could well suggest that civil defence is a sensible insurance policy.
- Decentralisation. Centralised, large-scale facilities are vulnerable to a number of threats, especially military attack, sabotage and natural disaster. The Japanese electricity supply system during World War Two was largely based on small-scale hydro plants and therefore virtually impossible to destroy by bombing.[17]
- Diversification. Having a variety of ways to accomplish the same purpose is one of the most effective ways to increase resilience. An energy system having some fossil fuels, some hydro, some biofuels, and some solar and wind-generated heat and power is resilient to most threats that might put any single system out of action. A long drought could threaten hydro supplies or a Middle-East war might interrupt oil imports, but the diversity would provide a cushion against the worst effects that would result from dependence on a single source.
- Self-reliance. As distinct from self-sufficiency, self-reliance implies being able to get by with one's own resources if necessary.[18] It would

mean using imports, outside experts and assistance to some degree, but not becoming entirely dependent on them. For example, rather than using imported goods whenever they are cheaper, an attempt would be made to rely on local production in areas where this would foster skills and facilities that otherwise would be lost or not exist.

- Flexible skills. Development of specialised skills to produce products for narrow market niches may fail to provide the general skills which would become essential in a crisis situation. For example, manufacture of specialised chips in Australia is a poor way to provide either the technological infrastructure or the skilled labour to produce a basic computer should imports be permanently interrupted.
- 'Simpler' systems. Technological systems which are easier to construct, easy to repair and available for nearly anyone to use are generally more resilient to a variety of threats. For example, bicycles as a form of transport are less susceptible to interruptions of oil or steel. A food supply that includes a sizable component of local organic gardening is less susceptible to disruption than large remote monocultures dependent on pesticides and fertilisers. The criteria for 'simple' technological systems are not fixed, but depend on the technological and social infrastructure, including skills and availability of basic tools.
- Participation in planning. If many members of the public are genuinely involved in the process of technological choice, it is more likely that the technologies which are introduced will be those which are generally accepted. Furthermore, involvement by a range of interest groups makes it less likely that particular threats will be overlooked. If the promoters of the Australian Animal Health Laboratory had involved farmers in the decision-making process from an early stage, the massive problems encountered later might well have been avoided, either by reaching a different decision or by the farmers deciding to accept the laboratory.

These possible responses to the problems of technological vulnerability do not have a single common theme. Direct planning can be a narrow and specific type of preparation, whereas most of the other responses aim at a more general resilience. Some responses can be based on increasing the capacity to build and maintain sophisticated technologies; for example, increasing the capacity to build advanced computing facilities is quite compatible with the responses of self-reliance and flexible skills. On the other hand, some of the responses, such as 'simpler' systems and decentralisation, are more in tune with the principles of 'appropriate' or 'alternative' technology. Many of the approaches can be considered to be alternatives to large-scale, capital-intensive and often potentially dangerous technologies which become 'entrenched' both as physical artefacts and organisational arrangements, and which are vulnerable to a variety of threats due to their extreme inflexibility.[19]

While in the literature of technological risk there is well warranted attention to technological design and the social factors associated with it, the category of technological vulnerability points towards responses of 'social design', namely different ways of organising society and the technological systems embedded in it.

POLICY IMPLICATIONS

The vulnerability of technologies to major but unlikely threats is not a popular topic of analysis and action for policy-makers. Those who are promoting new technologies have little to gain by pointing out vulnerabilities, since this may seem to encourage or aid opposition. For example, the proponents of nuclear power have seldom mentioned its vulnerability to military attack, though such attack would be quite likely in the event of war.[20]

In many ways, an explicit concern about vulnerability constitutes a challenge to prevailing trends in technological choice. As the world market becomes more integrated, the self-reliance of national and local economies is reduced. The proposed world car, for example, with different parts produced in different countries, lowers the local economic resilience of any one of the participants. Electrification and computerisation proceed unabated, making societies more vulnerable to disruption of central electricity supplies and key computer part suppliers.

The market does not promote resilience in any regular or efficient way. It does promote certain types of resilience, such as the shift towards flexible specialisation, which some see as a result of increasing 'turbulence' in the economic system. But there is no preparation for certain extraordinary threats, such as the electromagnetic pulse. The process of social disaffection is another 'problem' not dealt with by the market, since by its nature disaffection is expressed through political channels rather than, or as well as, economic ones.

In Australia, the current encouragement of export industries aimed at market niches is a prescription for high vulnerability. Any highly specific industry is less able to respond to suddenly changed conditions and requirements. Specifically, aiming mainly at exports means that self-reliance is reduced. Essentially, the market niche approach is a high risk strategy aimed at reaping high profits. The other side of the coin, the chance of massive loss, is less often examined.

The process of 'rationalisation' in production also tends to eliminate the insurance value inherent in old systems. For example, as the steel industry scraps the less efficient technology of the open hearth, its capacity to respond to disruption in the newer facilities is reduced.

The issues of vulnerability and resilience in technological systems are not of overarching importance, but neither should they be totally overlooked; rather, they should become *a* consideration in policy-

making. Specifically, approaches which enhance diversity, decentralisation and self-reliance deserve greater attention and perhaps some degree of subsidy. One way to promote this is by involving a wider range of groups in decision-making. This not only reduces the risk of 'social disaffection' but also means that vulnerability issues are less likely to be overlooked, since diverse groups are less likely to coalesce unquestioningly around a single analysis and policy.[21]

NOTES AND REFERENCES

1. Pam Scott, 'Dealing with dissent: on the treatment of opposition to the Australian Animal Health Laboratory and the importation of live foot-and-mouth disease virus', *Search,* 19, 1, January/February 1988, pp. 6-9.
2. Charles Perrow, *Normal Accidents,* Basic Books, New York, 1984.
3. Wilson Clark and Jake Page, *Energy, Vulnerability, and War: Alternatives for America,* Norton, New York, 1981; Amory B. Lovins and L. Hunter Lovins, *Brittle Power: Energy Strategy for National Security,* Brick House, Boston, 1982; and James L. Plummer (ed.), *Energy Vulnerability,* Ballinger, Cambridge, Massachusetts, 1982.
4. Alan Borning, 'Computer system reliability and nuclear war,' *Communications of the ACM,* 30, 2, February 1987, pp. 112-131; Lance J. Hoffman and Lucy M. Moran, 'Societal vulnerability to computer system failures,' *Computers and Security,* 5, 1986, pp. 211-217; and Perry R. Morrison, 'An absence of malice: computers and Armageddon', *Prometheus,* 2, 2, 1984, pp. 190-200.
5. Richard Charles Clark, *Technological Terrorism,* Devin-Adair, Old Greenwich, Connecticut, 1980.
6. A. Barrie Pittock, *Beyond Darkness: Nuclear Winter in Australia and New Zealand,* Sun, Melbourne, 1987.
7. W.S.G. Bateman, *Australia's Overseas Trade: Strategic Considerations,* Strategic and Defence Studies Centre, Australian National University, Canberra, 1984.
8. Manuel Wik *et al.,* 'URSI factual statement on nuclear electromagnetic pulse (EMP) and associated effects', *International Union of Radio Science Information Bulletin,* 232, March 1985, pp. 4-12.
9. Paul Dibb, *Review of Australia's Defence Capabilities: Report to the Minister of Defence,* Australian Government Publishing Service, Canberra, 1986.
10. Paul Smoker and Morris Bradley (eds), *Current Research on Peace and Violence,* 11, 1-2, 1988, pp 1-79.
11. Wren Green, Tony Cairns and Judith Wright, *New Zealand After Nuclear War,* New Zealand Planning Council, Wellington, 1987.
12. Colin Kearton and Brian Martin, 'The vulnerability of steel production to military threats', *Materials and Society,* forthcoming.
13. Donald F. Barnett and Robert W. Crandell, *Up from the Ashes: The Rise of the Steel Minimill in the United States,* Brookings Institution, Washington DC, 1986; and R.D. Walker (ed.), *Small Scale Steelmaking,* Applied Science Publishers, London, 1983.
14. Walter H. Goldberg (ed.), *Ailing Steel: The Transoceanic Quarrel,* St. Martin's Press, New York, 1986, p. 464.
15. John Woodward, Chairman, Commissioners of Inquiry for Environment and Planning, *BHP Steel International Group Rod and Bar Products Division Proposed Steel Mill, Rooty Hill,* Report to the Honourable David Hay, Minister for Local Government and Minister for Planning, Sydney, May 1988.
16. M. Anjali Sastry, Joseph J. Romm and Kosta Tsipis, *Nuclear Crash: The US Economy After Small Nuclear Attacks,* Report #17, Program in Science and Technology for

International Security, Massachusetts Institute of Technology, Cambridge, Massachusetts, June 1987.
17. Lovins and Lovins, *op. cit.*
18. Johan Galtung, Peter O'Brien and Roy Preiswerk (eds), *Self-reliance: A Strategy for Development,* Bogle-L'Ouverture, London, 1980.
19. David Collingridge, *Technology in the Policy Process: Controlling Nuclear Power,* Frances Pinter, London, 1983.
20. Bennett Ramberg, *Destruction of Nuclear Energy Facilities in War: The Problem and its Implications,* Lexington Books, Lexington, Massachusetts, 1980.
21. Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascos,* Houghton Mifflin, Boston, 1983.