Management of Critical Strategic Infrastructure

John McCulloch B.Sc., M.Sc., F.Inst.M.&C., C.Eng.

Critical strategic infrastructures comprise those systems, which, when they fail even for a short period, our whole society suffers a significant and unacceptable degradation to the quality of life, not just at the time of failure but for some time after.

A clear instance occurred recently when an upgrade to a widely used computer operating system failed. Effects included: widespread train and flight cancellations, cancellations of hospital appointments including surgical operations and cancer treatments, bank cash machines unavailable, shops unable to take card payments, (some people went without food for a day or two because of the combination of the last two), mobile phone services disrupted and many other examples throughout the world. This operating system is clearly a global critical strategic infrastructure.

On a smaller scale, the UK Post Office Horizon system has caused Post Office managers to be falsely accused of fraud, to be forced to repay large sums of money that was not owed, to be convicted of fraud and imprisoned, to go bankrupt and to commit suicide. Some Post Office customers lost huge amounts of savings that could not be recovered.

Another event occurred recently in Europe, which emphasised the critical strategic nature of the electricity grid. Here, enough bolts were removed from an electricity grid transmission pylon to cause it to collapse. This resulted in several large conurbations being without any electrical power for several days. This was attributed to vandalism. I have removed scrap metal from a small, disused pylon. The effort required was huge, and it took several hours to remove about a dozen bolts that were not under any load. I estimate that a team of about six people well equipped with very heavy tools, (including sledgehammers to knock out the last few bolts supporting the weight of the cables), would have taken several hours to fell this pylon. I wonder if this was a test of the vulnerability of this infrastructure by a hostile power or an extremist organisation. There have also been some deliberate fires under transformers in electricity substations that may have been part of the same tests of vulnerability.

Strategic infrastructures include:

- Water and sewerage systems
- Public transport: bus, rail, ferry and air
- Roads, cycle paths and footpaths
- Canals and canal networks
- Banks and banking systems including credit and debit cards systems
- Electricity and gas supply and distribution networks
- Communication networks: paper-mail, telephone, mobile phone, Internet
- Health Services
- Shops and supermarkets
- Diesel, petrol and other portable fuel supply and distribution
- Rivers, lakes, flood-plains and marshy ground, (because of their impact on flood risk)
- Waste recycling, disposal and landfill

- Housing
- Education at all levels
- Information media: newspapers, radio, TV and Internet

It is important to recognise that these infrastructures are not independent but interact in many and complex ways. For instance, a failure in the railway system will put additional load onto the road network. All decision-making must take these interactions into account.

Management of all of these infrastructures increasingly depends on computers and the software that enables them to provide support for these critical tasks. Computer operating system and network failures, therefore, can simultaneously threaten many of the items on the above list across several countries and so are global critical strategic infrastructures. The global positioning satellite systems must also be considered as global strategic infrastructures.

All of these infrastructures are clearly strategic targets in time of war and likely to become potential targets for hostile extremist organisations at any time. They are also vulnerable to accidents and natural events: weather, earthquakes, coastal erosion and human error. Their security and vulnerabilities need to be managed in this context as part of the overall structural design.

For management of these strategic infrastructures, the management organisation needs a clear understanding of the different uses to which the infrastructure is used. As an example of this, I want to relate my company's experience when windows-type operating environments first appeared. My company operated petrochemical and oil refining plants that required complex control systems; there are obvious risks if the control systems go wrong. The manufacturers of the control systems saw the windows environment as a technology that they wished to exploit. At that time, windows systems would often hang up for many seconds whilst performing obscure internal housekeeping tasks, and from time to time would crash without warning. Representatives of my company started to engage in talks with the windows system manufacturers about our time-critical and safety-critical control requirements and it quickly became apparent that there was very little appreciation of our needs. For this reason, it was over a decade before my company used a windows-based system for any safety-critical process control application.

Here it is clear that the management of the design of hardware and software was very distantly separated from both the management of the implementation and the use of the control equipment. There was no real appreciation by the manufacturers of the safety and reliability implications of their way of doing things. For any critical strategic infrastructure, there needs to be a full investigation of the requirements of the system. For any such infrastructure there will be many and diverse users and uses and a failure to generate a fully comprehensive statement of requirements, and to keep this updated as new uses develop and are exploited, will expose users to previously unknown vulnerabilities; accidental events will expose these vulnerabilities in new and unexpected ways. Even without such accidents, hostile minds could and do explore and exploit such vulnerabilities: computer ransomware, for instance.

The Post Office Horizon system is an excellent example of the failure to generate a comprehensive statement of requirements (SOR) at national level. The manufacturer of the system was expected to do this as part of its contract. The only rigorous way to generate this document for such a system is to engage several independent teams of consultants, at least three, to investigate each of the many different ways that such a system may be used. Investigation should involve observing each kind of user working

with the current systems and taking notes. Consideration should be given to making the system future-proof by considering probable and possible future developments of use. Once these investigations are complete, each of the teams writes its own SOR and then they all meet to compare notes. Different teams studying the same type of users will come to different conclusions, and they need to generate a single SOR for that type of user. The SORs for the different user types then need to be compared. Nothing is left out at this stage, but any conflicts need to be resolved to satisfy the needs of every kind of user without compromise. The management team and representatives of every type of user should check and approve the SOR at this stage.

Having generated a fully comprehensive SOR, a functional design specification, (FDS), then needs to be created. This will normally involve several potential manufacturers interpreting the implementation of the SOR using their own technologies. The FDS should consider: safety, reliability, maintainability, control, management, security, recovery from faults, vulnerability to hostile attack, vulnerability to accidents and natural events, human factors issues, user training and ease of use at this stage. Many of these considerations will require a degree of redundancy, (multiple independent systems so that a single fault cannot cripple an infrastructure), diversity, (different systems having the same functionality but independent implementation) and graceful degradation, (fall-back systems that will continue to operate at a reduced level of service when there have been failures). Future-proofing should be further considered at this stage by considering migration to different technologies as they develop.

The reader, having looked at the last two paragraphs, may be thinking that this can only apply to a new system and almost all critical strategic infrastructures are existing systems that are being developed and changed all the time: the road network, for instance, the electricity grid or the internet. Developments to an existing infrastructure fall into two categories. The first category is where the infrastructure is being extended in a way that lies within the pre-existing SOR and FDS principles. The second is where new technologies or departures from existing design principles are being considered, where there are new user types that are requiring additional SOR statements to cater for their needs or where operating experience has exposed previously unrecognised vulnerabilities that need to be addressed. Every example of the second requirement should go through the same design process including the updating and development of SOR and FDS, and for systems that have never been properly considered from this point of view, the whole process of development from scratch of the SOR and FDS should be done to discover what changes are required. It is always necessary to consider the whole system rather than the additional developments in isolation.

There is a particular problem here in the UK that applies far less to the other G8 nations: professional management qualifications in public office. All of the other G8 countries require a certain level of management educational qualifications for those making decisions at national level; the UK is alone in having almost nobody in public office with any formal management education or qualifications. Those that have any such qualifications obtained them in industry before taking a government job, and thus their qualifications are business orientated rather than specifically designed for public service. The UK is alone amongst these countries in that no UK universities currently offer any management courses specifically orientated towards management in government. At present, the UK would have to send all candidates abroad for education that is specific to their role.

The management of critical strategic infrastructure systems must clearly be done at a national level and requires an informed management with sufficient understanding of the technology involved as well as the strategic implications of the decisions made. This is clearly a government responsibility. This does not prevent the government

employing companies to perform investigations, implementation and maintenance of the specifics, but it does require the government team to have sufficient understanding of the technologies and their strategic implications to ensure that the companies involved are not exploiting the country and that the infrastructure continues to serve the best interests of the people.

Some of the infrastructures mentioned above have global implications. Management of these systems clearly need to be done globally by a team that is representative of all of the national governments affected by the decisions of this team. At the moment, this is done in a very ad-hoc manner. The United Nations has interests in world peace, world health and human rights but has no involvement with the Internet, world-wide computer operating systems, global positioning systems or the world-wide use of credit cards, all of which are critical global infrastructures. The United Nations needs to consider its involvement in these areas.