Chapter 5
Critical Information Infrastructure

The review of Critical Infrastructure so far gives a somewhat confusing picture. There is a lack of clarity between Critical Infrastructures and Critical Information Infrastructures in almost all documentation related to Critical Infrastructure. Although the terms are not used specifically in an interchangeable manner, it remains the case that there is a considerable amount of overlap in the use of the terms. However, a common list of what are termed Critical Infrastructures has been arrived at. They are complemented by Critical Information Infrastructure. This Chapter seeks to place Critical Information Infrastructure in its correct context.

It is important to understand the proportionality of Critical Information Infrastructure. By this is meant the importance relative to other Critical Infrastructures. One way of doing this is by understanding the dependency of Critical Infrastructures on Critical Information Infrastructure.

The Critical Infrastructures looked at have been, the common list, referred to earlier:

- Finance
- Energy
- Food Supply
- Health
- Government Services
- Law and order
- Manufacturing
- National Icons
- Transport
- Water
- Waste Water
- People
- Education

Each of these has a reliance on Critical Information Infrastructure to a greater or lesser extent. It is not necessary, here, to repeat the comments contained in the country reviews. Looking at the points already made about these infrastructures we can say that within the OECD these are more strongly linked to Critical Information Infrastructure than elsewhere, because Information Infrastructure is more prevalent in the OECD than elsewhere,

and it can be said that in the areas of Finance, Food, Manufacturing, and Transport there is total reliance on Critical Information Infrastructure. That this is so should be reasonably obvious.

However, for the sake of clarity it is worth pointing out that Finance depends on the electronic investment, commercial, and personal banking services to be maintained; food depends on the supermarket, and other outlets, reordering and "just-in-time" processes to function as a supply chain; manufacturing depends on a variety of Manufacturing Resource Programs to succeed and Transport depends heavily on electronic information, ticketing, and electronic control measures.

This is without necessarily introducing the Internet into the equation. All other Critical Infrastructures also have heavy dependence on electronic information systems. In many cases they are now dependent on Information Infrastructure; it is just that in these cases there is a possibility of returning to some form of manual alternative. This is not the case in Finance, Food, Manufacturing, and Transport. These infrastructures would simply not survive a collapse in the Critical Information Infrastructure.

Critical Information Infrastructure is proportionally more important than all other infrastructures because there is a dependence on Critical Information Infrastructure by all other infrastructures. It is important, therefore, to understand how well advanced the various parts of the Critical Information Infrastructure industry is in protecting itself and customers from this perspective. In doing this it is worth bearing in mind the approach of the Petroleum Industry. The American Petroleum Institute[103] and the UK's Institute of Petroleum (now the Energy Institute)[104] have developed a series of approaches and standards to their business that has, over time, made operation of electrical and electronic equipment "intrinsically safe" in hazardous petrochemical environments. The operation of Critical Information Infrastructure has similar demands in terms of an approach. As yet, most of this development is in private hands and not coordinated, except at an information level, by any national or international body.

Critical Information Infrastructure can be broken down into the key areas of connectivity, hosting, security, hardware, and software. The major countries also have official bodies looking at the performance of different related industries. In addition, a number of national and international mechanisms for developing public–private partnerships and the sharing of information have been established. A review of these activities in relation to Critical Information Infrastructure follows.

There is no international body specifically responsible for Critical Information Infrastructure. A number of international bodies with some concern for Critical Information Infrastructure have already been mentioned.

The International Telecommunications Union (ITU)[105] has responsibility at an international level for telecommunications – but this does not extend to the

[103] Available at http://www.api.org (Accessed: 6 January 2007).
[104] Available at http://www.energyinst.org.uk (Accessed: 6 January 2007).
[105] Available at http://www.itu.int/home/index.html (Accessed: 6 January 2007).