Chapter 3
Critical Infrastructures and Critical Information Infrastructures: Approaches by Geography

This review of Critical Infrastructures and Critical Information Infrastructures looks at the major issues from different geographical viewpoints. The purpose of this is to give some understanding to the issues and importance of the overall subject in a number of different countries. The key countries looked at here are the UK, the USA, Australia, and New Zealand. Europe is also covered in some detail. This is simply because in any literature search they are clearly leaders in this field.

In the USA Dr. Jim Kennedy of Lucent comments as follows:

It has always been the policy of the United States to ensure the continuity and security of the critical infrastructures that are essential to the minimum operations of our economy and government. This critical infrastructure includes essential government services, public health, law enforcement, emergency services, information and communications, banking and finance, energy, transportation, and water supply.

So even before the events of 9/11, the Executive Branch of our government, the President through Presidential Decision Directive 63 (PDD 63) issued May 22, 1998, ordered the strengthening of the nation's defenses against emerging unconventional threats to the United States, including those involving terrorist acts, weapons of mass destruction, assaults on critical infrastructures, and cyber-based attacks.

But how many of us really understand what an immense undertaking that was? What is the critical infrastructure in the United States?

- *More than 3,000 government facilities*
- *7,569 Hospitals*
- *Telecommunications: 2 billion miles of cable; 1000s of telephone switching central offices*
- *Energy: 2,800 Electric power plants; 300,000 oil and natural gas producing sites; 104 nuclear power plants*
- *Transportation*
  - *5000 public airports*
  - *500,000 highway bridges*

– 2 million miles of pipelines
– 300 coastal ports
– 500 major urban public transit operators:

• 4,893 banks or savings institutions have more than $100 billion in assets
• 66,000 chemical and hazardous material producing plants
• 75,000 dams
• 51,450 fire stations responding to 22,616,500 calls for assistance each year.

US business and every individual rely in some manner on the above every day. We depend on their operational resiliency and continuity of operations.

Initially, critical infrastructure assurance was essentially a state and local concern. With the massive use of information technologies and their significant interdependencies it has become a national concern, with major implications for the defense of our homeland and the economic security of the United States.

However, given all of the focus on critical infrastructure still one in three critical infrastructure operations goes without a business continuity or continuity of operations plan and three out of five of those operations with plans have never tested their plans as "fit for purpose."[30]

Clearly Critical Infrastructure and Critical Information Infrastructure is an important issue in the USA.

What Critical Information Infrastructure/Infrastructure is:

Critical Information Infrastructure is perceived as an essential part of national security in numerous countries today and has become the nucleus of the US terrorism and homeland security debate after 11 September 2001. A critical infrastructure is commonly understood to be an infrastructure or asset the incapacitation or destruction of which would have a debilitating impact on the national security and the economic and social welfare of a nation.[31]

In the USA, the important initiative and policy on Critical Infrastructure and Critical Information Infrastructures is the following:

Executive Order on Critical Infrastructure Protection

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

---

[30] Kennedy, J (2006) Critical Infrastructure Protection is all about Operational Resilience and Continuity, *Continuity Forum*, 17 November. Available at http://www.continuitycentral.com/feature0413.htm (Accessed: 6 January 2007).
[31] Dunn, M and Wigert, I (2004). op. cit.