Chapter 12
General Summary and Conclusions

Chapter 1

- Critical Infrastructure Protection is about Defense
- Critical Infrastructures need to be Resilient

Chapter 2

- Resilience is about the ability to "bounce back"
- Critical Infrastructure Protection is not the same as Critical Information Infrastructure Protection
- Critical Infrastructure Protection is essentially national; Critical Information Infrastructure is both national and "borderless."
- Both Critical Infrastructure Protection and Critical Information Infrastructure are inseparable from society's core values in a political, social, economic, and technological sense.
- There has been a migration of Critical Infrastructure from Government to Private hands over the last 50 years.
- Fewer resources are devoted to the Defense of Critical infrastructure than 50 years ago.

Chapter 3

- There is clear stated political support for Critical Infrastructure and Critical Information Infrastructure across all countries.
- There is less clear definition of actual operational support for the protection of Critical Infrastructures and Critical Information Infrastructures across most countries.
- A common set of Critical Infrastructures can be defined.
- Risk management is important.
- There are concerns with regard to the dominance of Information Technology in all Critical Infrastructures.
- There are legal gaps at international and national level regarding both Critical Infrastructure and Critical Information Infrastructure.
- Thought leadership in this subject area is not related to size of country or Infrastructures.

Chapter 4

- Every single Critical Infrastructure in the common list is under threat; none of them really display the characteristics of resilience.
- Governments are clearly not paying enough attention to Critical Infrastructures, and they are not properly prioritized neither in any national sense, not of themselves.

Chapter 5

- The Connectivity, Hosting, Security, Hardware, and Software industries combined, and in general, pay little heed to Critical Information Infrastructure protection.
- There are no major international, European or national bodies addressing the subject operationally in an effective manner, although some of the telecommunication bodies are trying.
- There are many Public–Private Partnership and Information Sharing Initiatives, but they tend to lack teeth.
- Some Information Sharing initiatives are effective, e.g., CERTS and WARPs, and work well from the bottom up, as in the New York State example.

Chapter 6

- The export of democracy has increased the threat to Critical Infrastructures, and led to the increased likelihood of Asymmetric and traditional war.
- There is demonstrable resilience in the Economic field, but this is balanced by a lack of Obstructive Marketing techniques outside of friendly western style cultures.
- Inequality and religion are the main social threats to Critical Infrastructures.
- Technical Developments are both positive and negative for Critical Infrastructures, with a view that the future balance may be negative.
- Global warming will have, at least in the short term, an almost universal negative effect on Critical Infrastructures.
- Legal and regulatory controls are on the increase for Critical Infrastructures.
- Risk management and the understanding of dependencies are increasingly important.
- Critical Information Infrastructure's primacy is confirmed.

Chapter 7

- In less than 20 years the use of Critical Information Infrastructure in business has advanced beyond recognition.
- Critical Information Infrastructure protection is now a key issue for business, led by the banks.
- Many standards across the regulated and nonregulated business have been introduced.
- These standards, including Sarbanes-Oxley, can be approached from a common base ISO 17999