# A Global Approach to Protecting the Global Critical Infrastructure

Dr. Stephen D. Bryen

# Scope of Problem

Study of 4,900 computer professionals in 30 countries shows immense losses due to computer attacks …

In the U.S. companies will buy $1.7 billion in security services by 2005 (up from $140 million in 1999)

# Types of Information Warfare

3 Main Classes

- Class I --Privacy Attacks
- Class II –Espionage (public & private)
- Class III– Terror attacks against Critical Infrastructure

# Nature of the Cyber Environment

- No borders or boundaries to defend
- Governments control only a part of the telecommunications/Internet environment
- Voluntary cooperation (at best)

# Critical Infrastructure

Concept put forward by President's Commission on Critical Infrastructure Protection (1996)and reflected in PDD-63 (U.S.) and Executive Order on Critical Infrastructure Protection in the Information Age ( October, 2001)

# Critical Infrastructure Elements

- Information & Communications (telecom, networks, Internet)
- Electric Power (conventional, nuclear)
- Transportation
- Oil & Gas (supply, transport, refining, distribution)
- Banking and Finance
- Water & Emergency Services
- Government (+military)
- Manufacturing (Japan)

# Lack of Success

- U.S. General Accounting Offices gives “failing grades” to government agency efforts to implement and protect networks, despite substantial funding plus ups
- August 2001 finds “significant and pervasive weaknesses” and “serious security problems”

# Defining the Threat

- Structured (group, organization, government)
- Well financed
- Is a hostile actor
- Actor protects its team
- Backed up by intelligence agency or agencies or equivalent structure
- Shares intelligence with other countries, terrorists

# Countermeasures

- Most solutions are technical. Most are product designs focused on “hackers” and not against structured hostile threat
- Today’s protective schemes include virus and intrusion detection, vulnerability testing, security patches, security policies
- Most schemes don’t protect well against insider threats (inside structured hostile threat)

# Poor Linkages in Security Protection Schemes

- Most technical solutions suffer from a *poor linkage* between current intelligence (both law enforcement and national means) and off the shelf (COTS) solutions
- Most U.S. government agencies buy COTS security products (including military)
- Many technical solutions fail to protect networks from “novel” attacks

# Linkages continued …

- Most commercial software takes a minimalist strategy toward security (e.g., Microsoft email/browser, Microsoft Office, Sun Java)
- Virtually all commercial software is designed by engineers and programmers who have no security background or threat briefings

# Current U.S. "Solution"

- Major funded initiative to enhance network security in government agencies
- Voluntary cooperation with private sector
- Effort to produce "government" (e.g., DITSCAP, HIPAA)security standards
- Limited international cooperation
- Not yet supporting ISO17799 (British Standard 7799)

# An International "Solution"

- Cooperation in setting technical computer and network standards
- Formal certification and accreditation system applied to networks and security products
- International coordination in intelligence gathering, law enforcement

# International "Solution" Underpinnings

- Agreement on common critical infrastructure model
- Trust and confidence building
- Active government participation at policy level
- Collective Security

# Collective Security

A collective security agreement among the infrastructure stake holder countries

An attack against the infrastructure of one is an attack against all and member states are obliged to cooperate fully to intercede against the source of the attack

# Is it Possible?

Thinking ahead –

- ✓Start with a limited experiment to protect collectively telecommunications networks and military networks
- ✓Expand if warranted to other parts of the critical infrastructure

# Elements of the IO

- Member States political representatives supported by technical experts and commercial firms
- A Charter reflecting the collective security responsibilities of the Members
- A Secretariat and Staff to manage high level meetings and the IO's committees

# Elements of the IO

- A Secretary General of high rank to provide leadership and continuity for the IO
- Agreement to safeguard sensitive and timely information and means to secure information
- Vetting of staffs (reciprocal)

# Organization

- Cyber Warning Center to coordinate intelligence about possible cyber attacks and identify probable origins of attacks
- Legal Affairs Coordinating Center for laws enforcement initiatives
- Business and Industry Cooperative Forum
- Technology Security Committee