

# **Information Warfare: From Security to Infrastructure Protection to the Military**

## **An Overview of Security, Electronic Civil Defense and the Networked Society**

Ever since Assistant Secretary of Defense John Hamre in April 1998 and July, 1999 declared ““We Are At War”, the media has stood up and noticed.

Cyberwar. Infowar. Netwar. These are all different flavors of a conflict between adversaries without bombs, bullets and bayonets. Way back in 1991, your seminar leader Winn Schwartau coined the term Electronic Pearl Harbor and warned Congress that our computers were poorly protected against an adversary.

This unique session will enlighten you, entertain you and just maybe scare you. You do not need to be a technocrat or a bureaucrat to understand that Info was preordained by the very nature of the technology around us. Our absolute reliance upon technology (not just the Internet!) is not only our greatest asset but also our greatest vulnerability.

You will learn about all three classes of Information Warfare: Personal, Corporate and Global and how they evolved. What global causes and changes have occurred which make ideal conditions for Infowar? Who is waging info and why? How has the nature of global competitiveness and cultural diversity added to the impact?

This seminar is full of exciting interactive discussions, debate and videos to keep everyone awake for the whole day!

- Information Warfare: Definition
  - Information is both the Weapon and the Target
  - Replaces Conventional Warfare?
  - Military pre-eminence Insignificant?
  - A lot more enemies than ever before
  - Military can be effectively bypassed
- Financial Conflict?
- Convergence of Military and Civilian Interests
- Defensive Policy
  - Convergence: Military and Civilian

- New Global Economy and InfoWar
- Competing Spheres of Capitalism
- Computers Everywhere
  - Commercial Sector is the Battlefield
  - Infrastructure Convergence
- Cyber-Crime & Cyber-Terrorism
- Detection/Reaction
- Personal Privacy
- New Society on the Horizon
- Globalization of Economies
  - Society is Going Flat
- Class I: Personal Information Warfare: In Cyberspace: Guilty Until Proven Innocent
- Class II: Corporate Information Warfare: More Spying Than Ever
  - 122 Countries w/ on-line espionage capability
- Class III: Regional or Global Conflict: Electronic Pearl Harbor
- Transport Layer w/o Redundancy
- Malicious Software (Viruses, embedded code)
- Chipping
- Hacking
- Sniffing the Net (Cell phone, telco, fax)
- Social Engineering
- PsyOps & Perception Management
- Electromagnetic Eavesdropping
- Denial of Service Attacks
- Magnetic (DEW) Offensive Assaults
- Hacking Statistics
- Social Engineering
- Sniffing the Net
- Electromagnetic Eavesdropping
- Confocal Vulnerability
- Nuclear Weapons of the Information Age
- Who Are the Information Warriors? Motivation
- Political Infowar Events

- US Based Terrorism
- Cyber-Civil Disobedience
- When is an Attack Worthy of Response?
- What constitutes an attack?
- Law Enforcement
- Graceful Degradation
- Electronic Bill of Rights
- Resources

**Prerequisites:**

A general technology user with minimal technological skills will get a great deal out of this seminar. An appreciation and understanding of history, politics, finance and current events will make it all that more enjoyable.

**Reading:**

The seminar leader, Winn Schwartau has written the three seminal works on Information Warfare. The most recent version is available from bookstores or on-line.