Information Warfare

The Weapons of Intelligence and Conflict in the Information Age

Winn Schwartau
Interpact, Inc.
11511 Pine St.\ Seminole, FL 34642
V: 813.393.6600 \ F: 813.393.6361
Http://www.Infowar.Com \ Email: Winn@Infowar.Com

Information Warfare: My definition in 1993

- A conflict where the use of information and information systems are used to compromise,corrupt or destroy the information and information systems of one's adversary.
- The Migration of Conflict To Commercial: Convergence
  - Replaces Conventional Warfare: Military pre-eminence outmoded?
  - No longer necessary for a military conflict
  - A new dimensiion without bombs and bullets
  - Prelude to Conflict /Lethality Reduction
  - The world is moving so fast these days that the person who says it can't be done is being interupted or passed by the person who is doing it. I hope to have put myself in that position.
  - Declassify the Threat
- How does any country defend itself against an attack? Electronic Pearl Harbor

Governments Need to Understand

- IW Can Be Waged By Anyone
- Open Source Intelligence
  - No More Secrets
- What's available to me/us, is available to them
- Commercial Infrastructure weak, unsecure.
  - Military requires commercial infrastructure
  - Technology Proliferation
- Borders are meaningles
- A lot more enemies than ever before
- Military can be effectively bypassed
- Enemies can be invisible and unidentified
- National Convergence
  - Military and Civilian Interests

hh

New World Order of Economic Competitiveness

- Three Spheres of influence with differing approaches to capitalism
  - North America
  - Europe
  - Far East ("Business in War")
- New targets abound
  - Third World and Agrarian/early industrial age adversaries

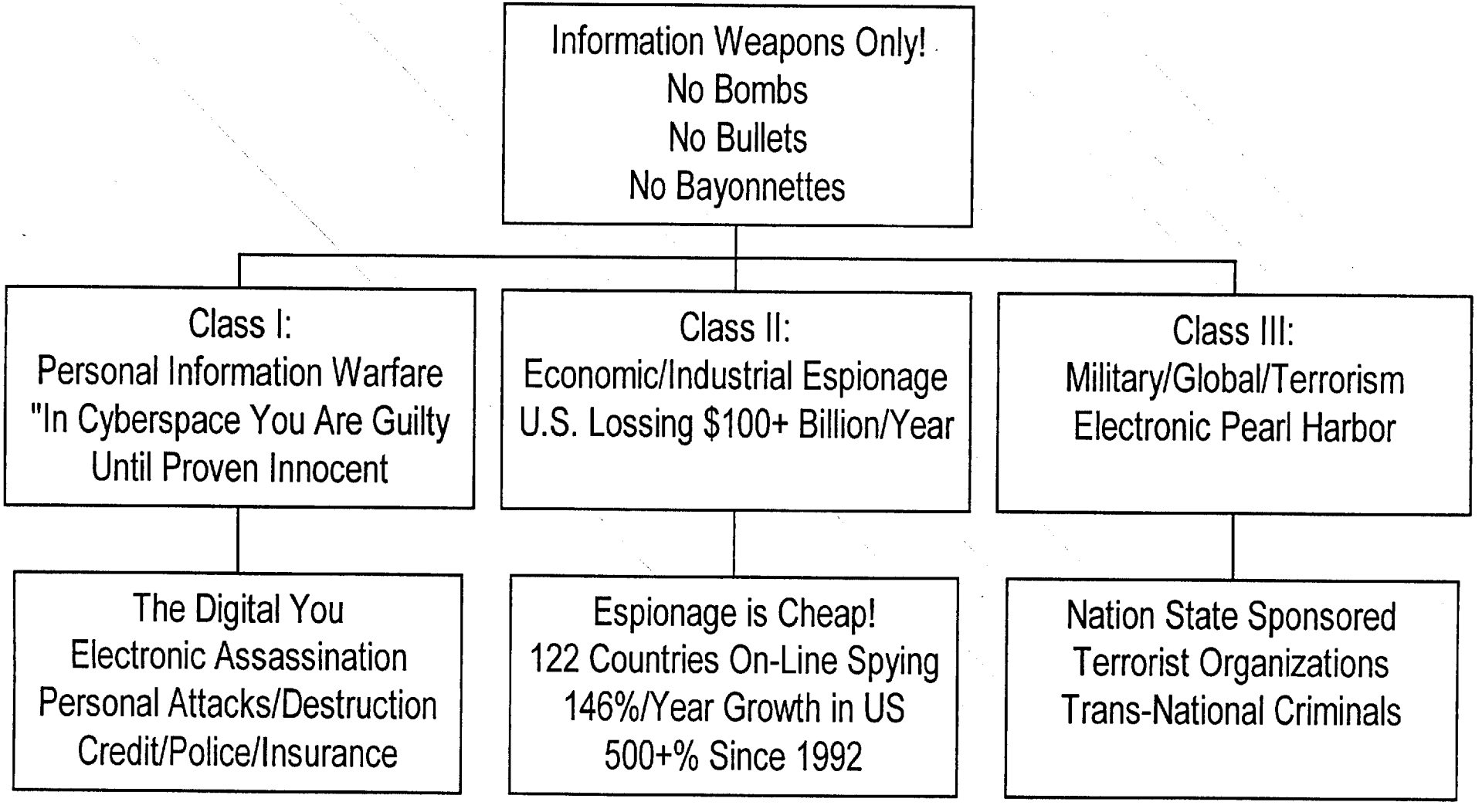
Computers Everywhere and the Global Network

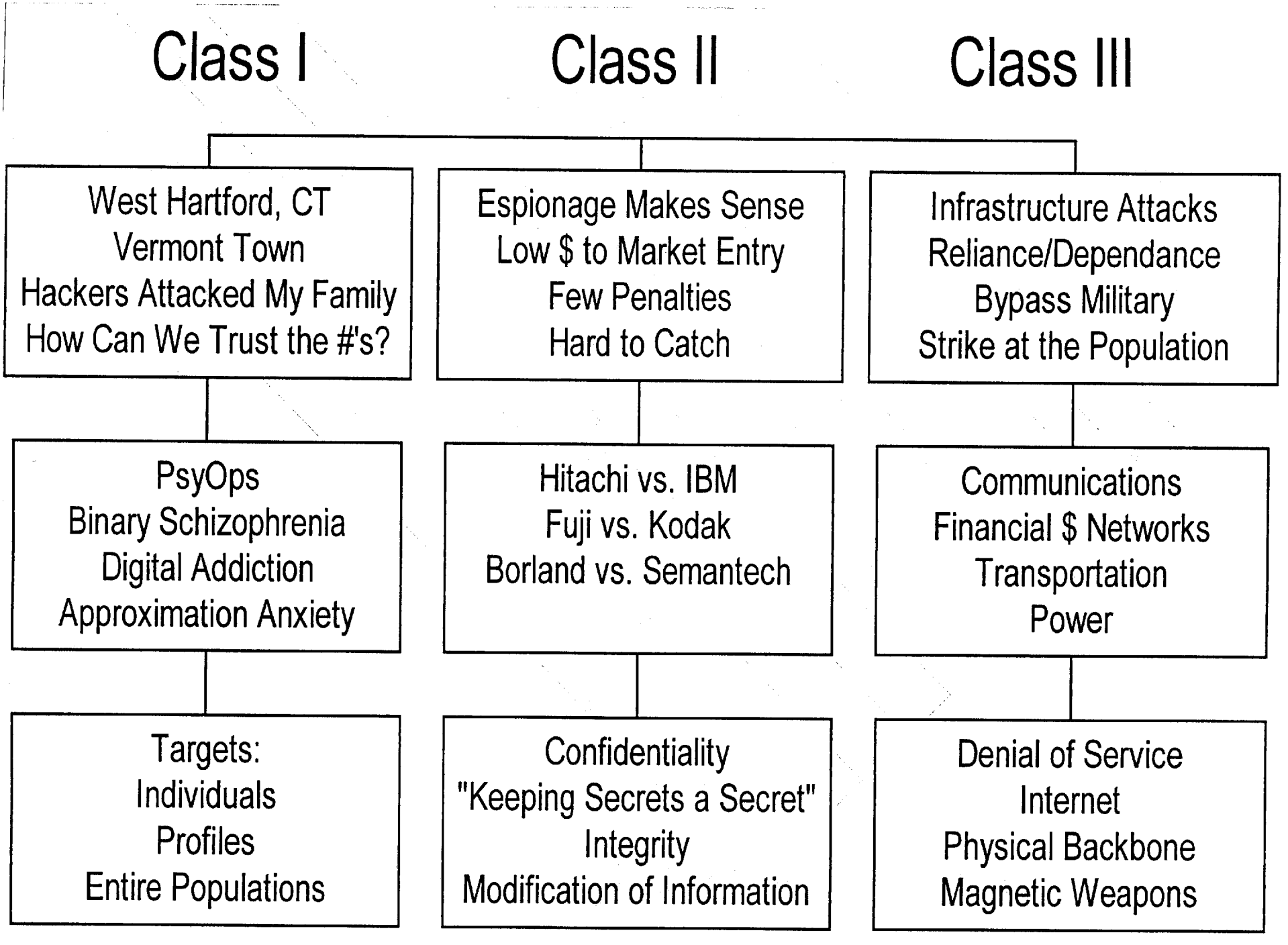
- 3 Spheres of Capitalism
  - Economic Competitors replace Military
  - Military Allies = Commercial Competition
- Econo-technical Infrastructure is the target
  - Finance: Corp/Personal -
  - Transportation
  - Power Distribution
  - Communications
  - Complexity Breeds Vulnerability - ergo - that which gives us the advantage also is our greatest vulnerability
- Commercial Sector is the Battlefield

Defensive Policy

- For decades we based have our defensive posture upon our adversaries capabilities, not their presumed intentions.
  - I suggest that we currently have no policy to defend the US against a concerted enemy Cyber-attack
  - Corporations need new definitions and charters.
- All of our economies and domestic econo-technical infrastructure is a strategic national security asset worthy of protection.
  - Should we sacrifice it for the sake of military secrets?

The 3 Classes of Information Warfare





Information Weapons Goals: same for THEM as for US

- Goal dependent
  - Anonymous
  - Invisible
  - Passive
  - Insidious
  - Effective
  - Available
  - Inexpensive
- Attack the Fundamentals
  - Integrity
  - Confidentiality
  - Denial of Service (Availability)

Weapons for the Information Warrior: PsyOps in Cyberspace

- Manipulate the images - sounds - ideas
  - Perception Management
  - ie, Somalia
  - New Sarnoff Tools
- Data Bankers
- Hacking
- Public Records
- Social Engineering
- Media
- Attack the Social Malaises of the population

Anonymous Financial Transactions

- Criminal Central
- Use Tools of Today
- Electronic Bank
- No Names
- Sender/Receiver
  - Know each other
  - Exchange Keys
- "Bank" commission
  - Establishes Trust

Soft Weapons for the Information Warrior

- Malicious Software -
  - Bots - Viruses - Trojan Horses
  - Modified Applications for military offense
- Software is inherently error-prone - Goedel
  - Bank of New York
  - Chicago Bank
- Exploit the weaknesses
  - Technical
  - People

Malicious Hardware - Chipping

- Import: How do we know it/they will operate as advertised?
  - Keyboard, BIOS,
  - Already happening
  - Iraqi Virus Hoax
  - Pentium debacle"
- The only difference between a programming error and malicious software is intent!

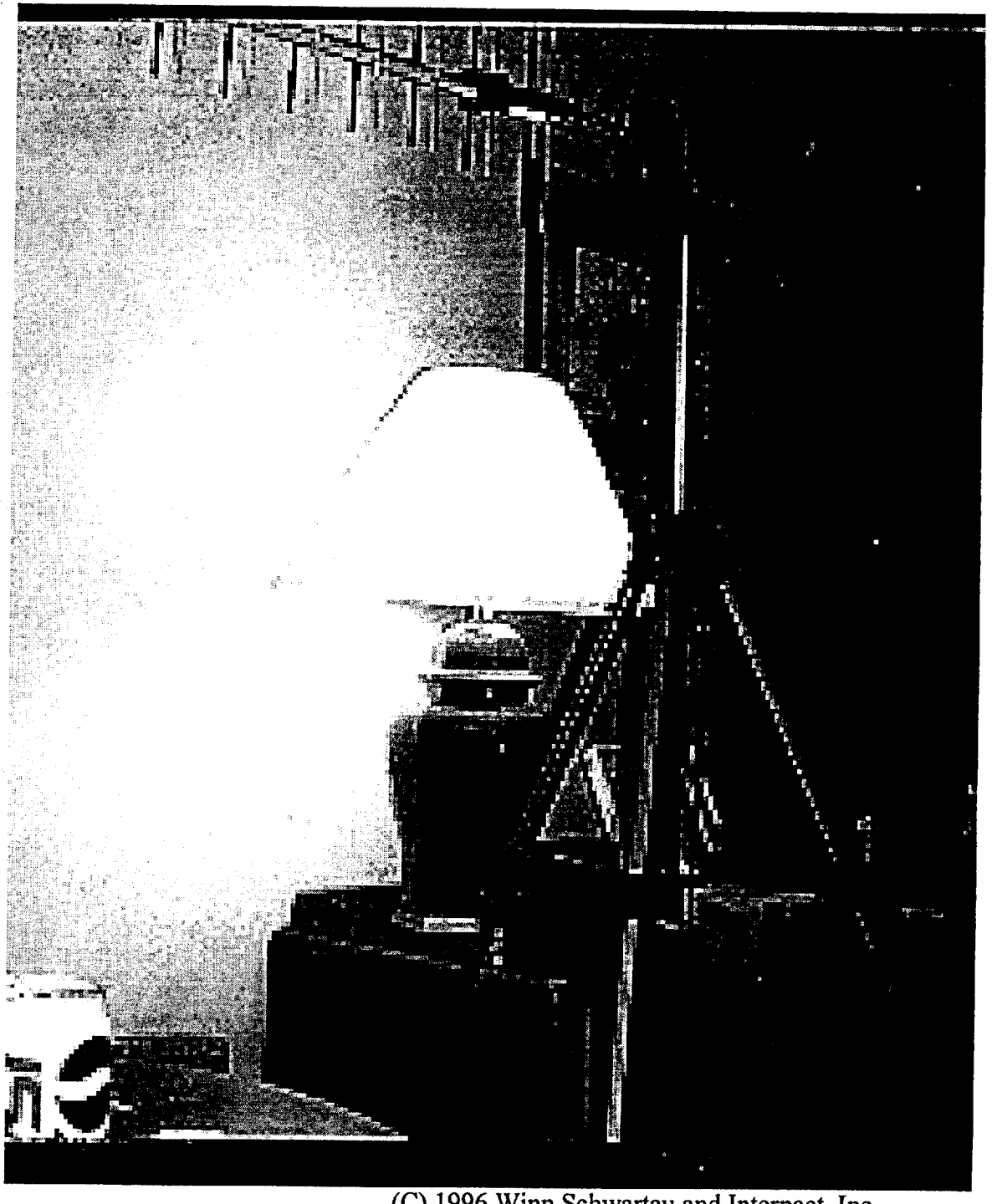
Hacking

- Anonymity - Amateur or Professional Hacking
- DISA - 1/399 MI 1/1000
- "Hackers are a national resource to be cultivated, not persecuted."
  - Netscape - Three Times in Three Months
- Hacking as National Resource
  - Amoral Sociopathic Scum?
  - Early Warning Radar System for Cyberspace?
- Counter-Culture of the 1990's; Remember the 60's!
- Do they have a place in national security?

Sniffing the Net

- Interception
- Eavesdropping
- Internet
- PSN's
- Voice
- Cellular
- FAX
- Satellite
- Buy/Acquire the tools for free (The Internet)

Cellular Hacking



Electromagnetic Eavesdropping

- Tempest Busting Once a secret
  - Van Eck Papers 1985,
  - BBC 1989 - Moeller 1990 - Geraldo 1991 - No. CA Chemical Co. 1990 - Chemical Bank 1993
- Power Lines, Ground Signals
- Home Brew for less than $50

Why worry about Denial of Service?

- Confidentiality and Integrity Solved
  - Virus and WORM Events
- Tech based orgs: comm and mil
  - Soft kill
  - Civilian Government : Unclassified Military
- Banks - Retail Presence <50% in 6 years: Prime Victim
  - Apply to Future
- Double Whammy - World Trade Center - 1993 : No-name Storm of 1993
- "We have the Acts of God thing down. What about the Acts of Man?"

document.Bomber.JavaScript_MailBomber_Says.value = ""; } // End of hiding our code -->

This is a fully **FUNCTIONAL** harrassment tool. Use this at your own risk. Many system administrators find email bombing **VERY ANNOYING** *(but don't let me discourage you)*.

This works *most* of the time but like all code there is plenty of room for error so I don't promise any thing.

WARNING

This only works with Netscape 2.0 not 2.1 or 3.0 sorry!

don't forget to configure Netscape to your mailhost!!

User to Harrass *(user@host)*:

How many email bombs would you like?

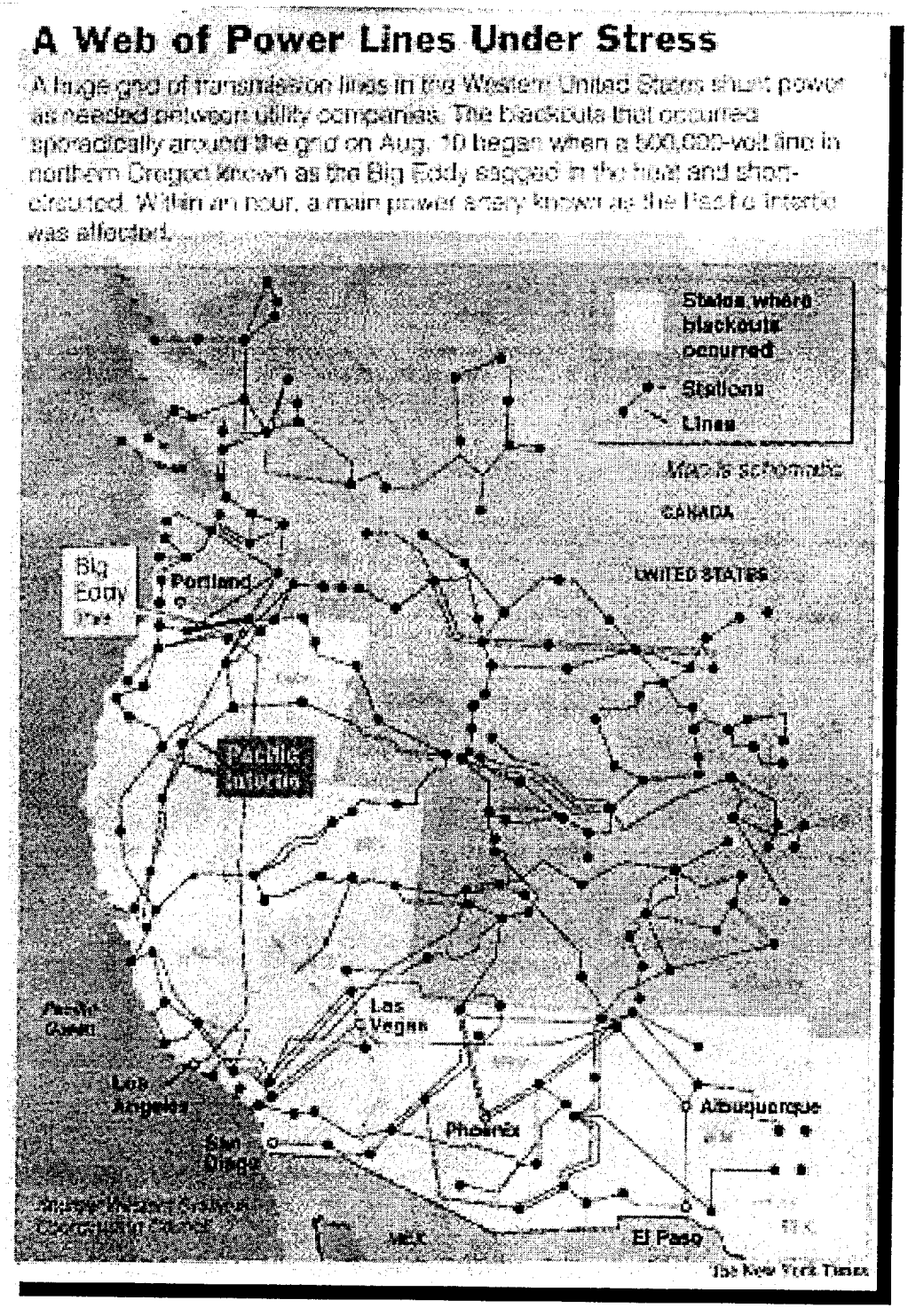
1000

Subject:

Your Terrorist Demands:

The Physical Transport Layer

- Velociraptor
- Comm
- Banking
- Backhoes
- Collapse
  - China
  - NY => Israel



The Western Power Grid: Part of the Critical Infrastructure

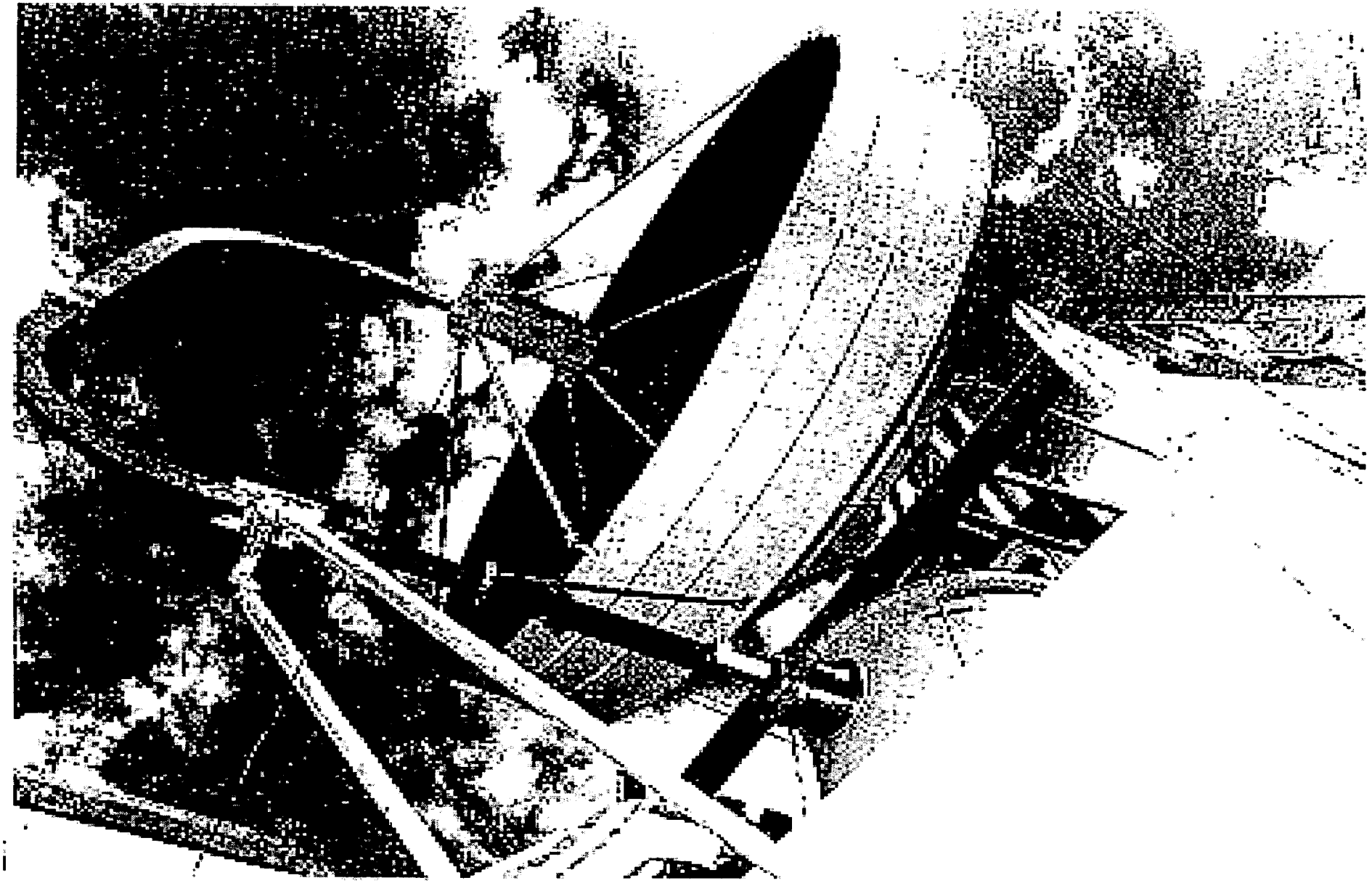
Large Scale DOS Events of Note

- Newark Airport - Power and backup power in same conduits
  - 24 Hour collapse & world-wide
- Air Traffic Controls
  - New York Airports -All 3 closed by fire in phone switch
  - 23 major events in 1995
- Telephone Companies
  - 1990, 1991
- Alleged Financial Attacks with stolen US weapons: 41 in Europe and US

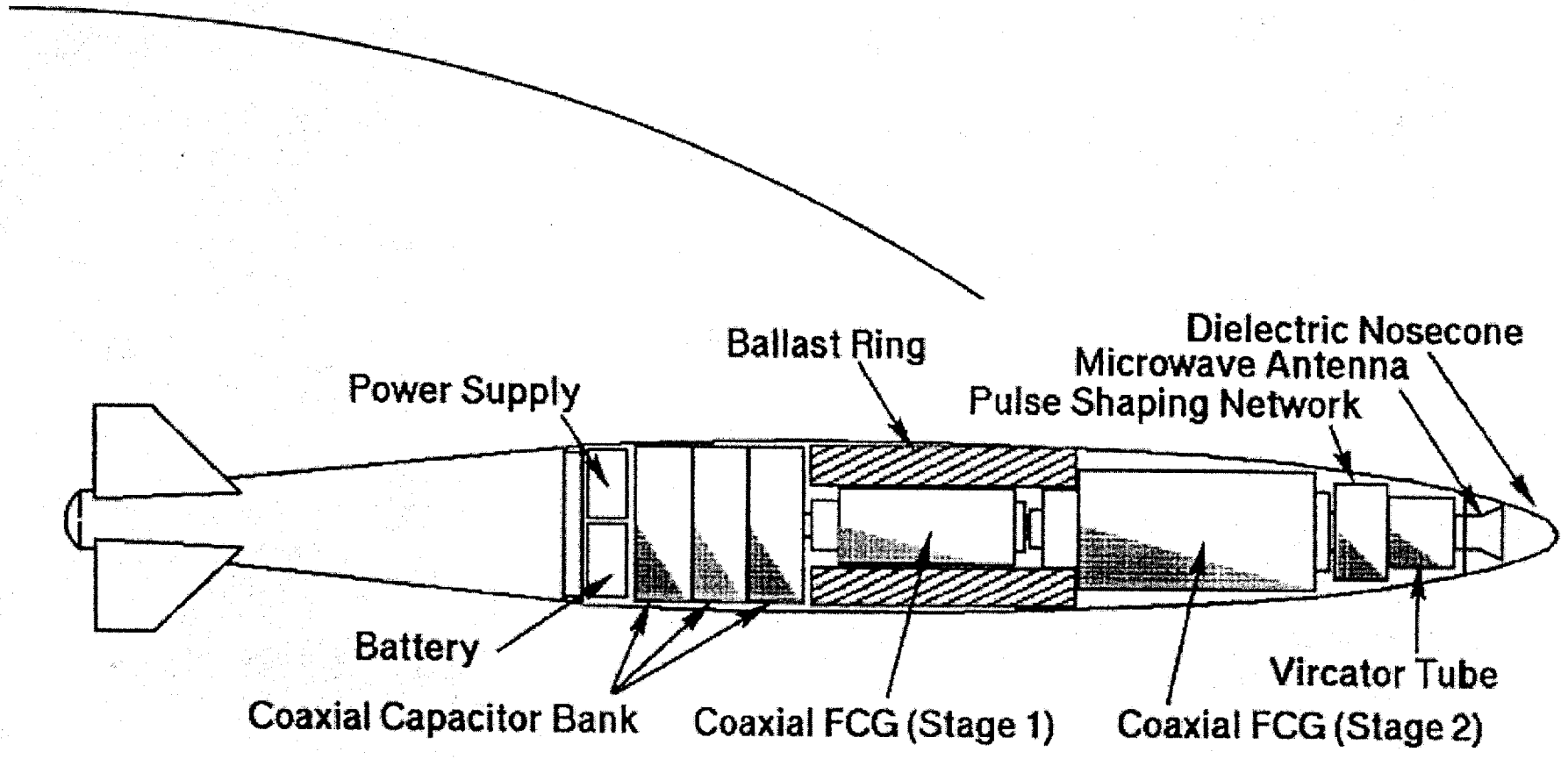
Nuclear Weapons of the Information Age

- Highly Classified - DEW
- HERF Guns - High Energy Radio Frequency
- EPC - Electromagnetic Pulse Cannons
- EMP/T Bombs - Electromagnetic Pulse Transformer Bombs
- HPM -High Power Microwave
- Congressional Committee who had never heard of these weapons.
  - Gulf War Use
  - HERO - Above air non nuclear - attack mil weapons with electronic vulnerability

Military HPM/EMP >10-100 GWatt



U.S. Military EMP: Cruise Missile/HA Bomb

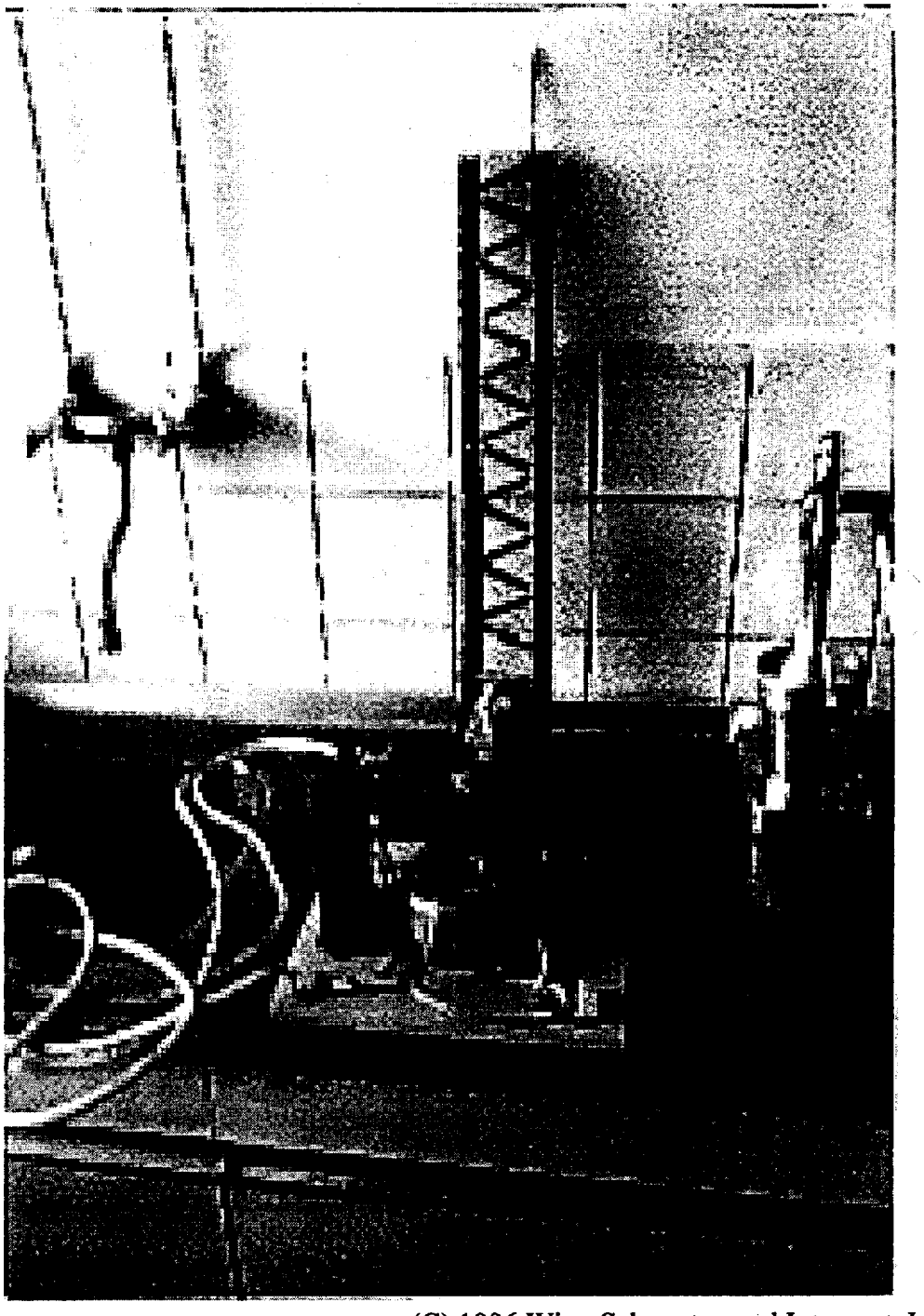


HIGH POWER MICROWAVE E-BOMB – GENERAL ARRANGMENT MK.84 PACKAGING
WARHEAD USING VIRCATOR AND 2 STAGE FLUX COMPRESSION GENERATOR

FIG.6 HPM E-BOMB WARHEAD (Mk.84 FORM FACTOR)

Home Made HERF/EMP Device

20MWatts
100 Ft. Soft Kill Range



National Information Policy

- Electronic Civil Defense
- Info as a Third Wave Asset and projection of power
- A Constitution for Cyberspace
- Create International Cyber-Borders?
- Federal/State Cyber-Borders?
- Information As Strategic Asset
- Should We Spy On the World?

National Solutions

- Acceptance of responsibility
- Argue/Lobby for smart legislation
- Declassify the Threat
- Get Commercial Help
  - Training/Awareness
- Reconsider old jurisdictional issues
  - No borders in Cyberspace

Electronic Bill of Rights

- Own Your Own Name
  - And associated information
- Organizations Must Protect Your Name and Info
- Notification of data
  - Right to Access
  - Right to Contest
  - Right to Remove
- New Gov't Classification
- No Local Ordinances
  - TN vs. CA Porno Case

What constitutes an attack?

- Hussein against
  - Attacks a Mil base in Europe or US
  - Blows up Statue of Liberty
  - Blows up a sports stadium (no loss of life)
  - Steals $267 from CitiBank
- What are proper responses?
- Who matters?
- Who decides?
- Where is the policy and leadership?

Closing

- New Paradigms
  - Is the economy a strategic asset of any country?
  - Do countries want to remain globally competitive?
- The Future has to Happen
  - So, do we want to adapt new thinking and understand new weapons to reflect the new realities of the 21st. century?
  - Chinese Proverb: If we don't change direction, we'll end up where we're going.

Netscape - [Information Warfare and INFOSEC]

File Edit View Go Bookmarks Options Directory Window Help

Location: http://www.infowar.com/index1.htm

What's New! | What's Cool! | Handbook | Net Search | Net Directory | Software

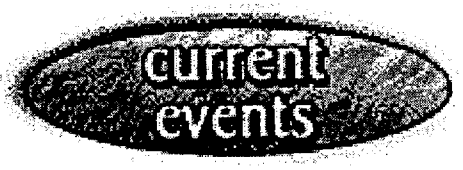

Class I
Privacy

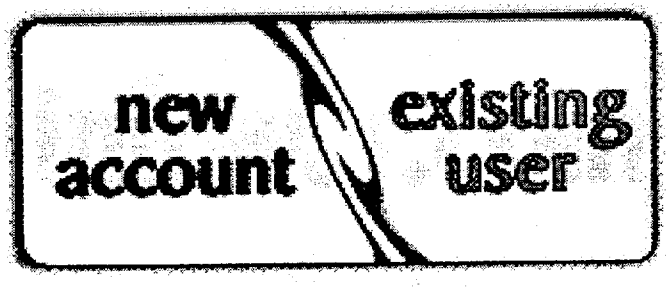

Class II
Espionage


Class III
Terrorism


Military & C4I


Hacker Musings





Reaching Us 

Discussion Groups 

Infosec
(coming soon) 

Chat
(coming soon) 

Search 

Document: Done

Open Source Intelligence: CONFERENCE Proceedings, 1997 Volume IV 6th International Conference & Exhibit Global Security & Global - Link Page

Previous	OSS '97 PROCEEDINGS Doug Tsuruoka, Asian Perceptions of What Is and Is Not Legal in Economic Intelligence Collection,
Next	OSS '97 PROCEEDINGS Bonnie C. Carroll, CENDI Information Managers' Group: A Brief Introduction,

Return to Electronic Index Page