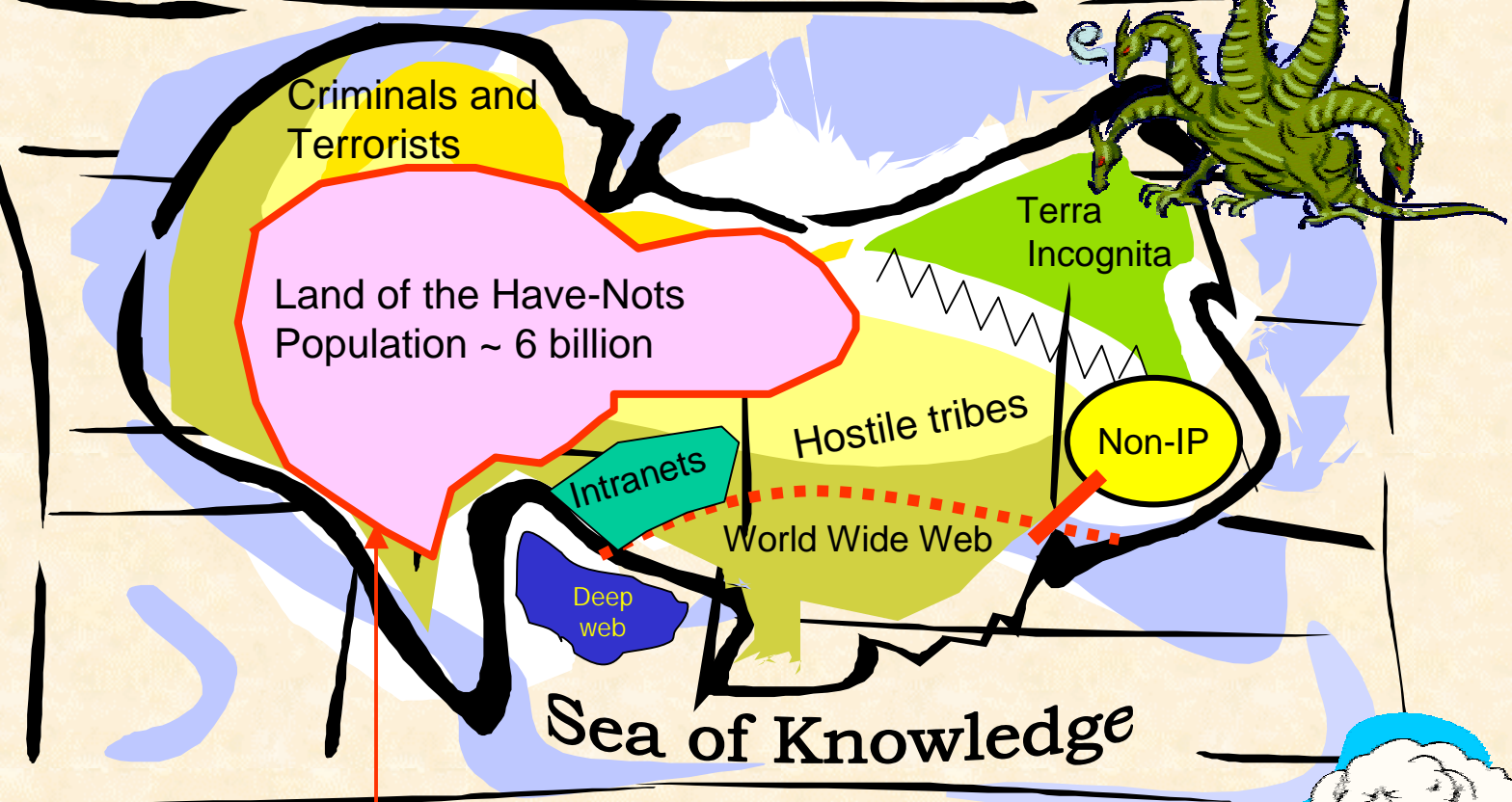


# CYBERSPACE



Sea of Knowledge

Digital Divide

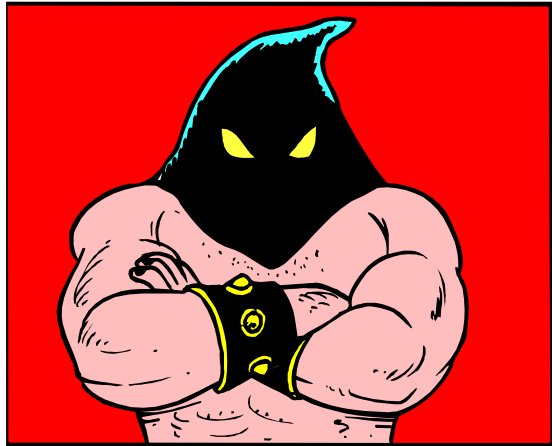
Explorers  
Navigators



  
*Cartografia Pietragialla*

# Crime and punishment

The “good old days”



Punishment was swift  
and severe

Now

U.S.A. 1995-2000

Kevin Mitnik, superhacker:

Arrested and sentenced to 5 years in jail

Fined US \$4,200

The Philippines, 2000:

Author of the “I Love You” virus

Arrested, released without charges

The Netherlands, 2001

Author of the “Anna Kournikova” virus

Arrested, tried, sentenced to 150 days  
community service

# The legal challenges

Traditional law is based on territorial boundaries

If cyberspace is the world of data and software,  
it is transnational and seemingly borderless

Whatever boundaries it has are porous and ill defined

Cyberspace enables transactions between people who do not know or cannot know the physical location of the other party

# Major areas for cyberlegislation

Human Rights related

Workplace related

Regulatory issues

E-commerce and  
Intellectual Property

Civil law

Criminal matters

National Security

Military use of cyberspace

Cyber-terrorism

Information Security Law

# Criminal matters

Fraud, sabotage, extortion, blackmail

Interception, modification and misuse of data and systems

Attempting, Aiding and Abetting cybercrime

Use of cyberspace by Organised Crime

Money laundering

Drugs, arms, slavery trade

Offshore unregulated gambling

Pornography

Anonymous networks and I Ds

# National Security

Telecommunications interception and analysis

Event monitoring in cyberspace

Roles and responsibilities of vendors and service providers

Encryption software

Search, seizure and rules of evidence

# Military use of cyberspace

Beyond the gathering of intelligence



What constitutes an act of war in cyberspace?

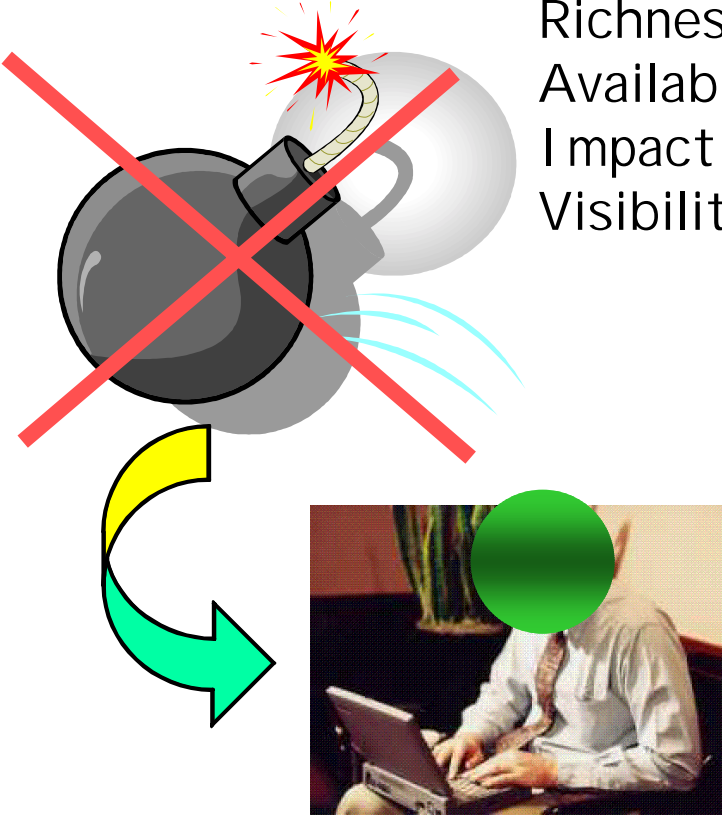
Can "information technology" be used as a weapon?

Rules of engagement?

Wait until it happens?

# Cyber-terrorism

WHEN, not IF



Richness of opportunity  
Availability and low cost of resources needed  
Impact of successful attacks  
Visibility

Ease of establishing global networks  
Ease of hiding in cyberspace  
Lack of legislation and jurisdiction



# International Legislation

OECD: 1983-1985 - Criminalization of computer abuse

Council of Europe (COE): 1985 - Work begins towards a convention on cyber-crime

United Nations - Congress on the Prevention of Crime

COE Convention on Cybercrime  
Signed in 2001 by 33 countries - not yet ratified

# International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime

The burgeoning of the world of information technologies has, however, a negative side: it has opened the door to antisocial and criminal behavior in ways that would never have previously been possible. Computer systems offer some new and highly sophisticated opportunities for law-breaking, and they create the potential to commit traditional types of crimes in non-traditional ways. In addition to suffering the economic consequences of [computer crime](#), society relies on computerized systems for almost everything in life, from air, train and bus traffic control to medical service coordination and national security. Even a small glitch in the operation of these systems can put human lives in danger. Society's dependence on computer systems, therefore, has a profound human dimension. The rapid transnational expansion of large-scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the opportunity for misuse or criminal activity. The consequences of computer crime may have serious economic costs as well as serious costs in terms of human security.

---

## CONTENTS

First issued in 1994  
Updated in 1997

---

## [Introduction](#)

- [The international problem](#)
- [Regional action](#)
- [The need for global action](#)
- [Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders](#)

## [THE PHENOMENON OF COMPUTER CRIME](#)

- [Definition of computer crime](#)
- [The extent of crime and losses](#)



Internet

# The COE Convention

Three primary groups of provisions

- Unauthorized computer intrusion, malicious code, the use of computers to commit acts which are already a crime
- Procedures to capture and retrieve on-line and other information by issuing "Retention Orders"
- Cooperation between signatory states to share e-evidence

Additional protocols are being developed

# Reactions to the Convention

33 States (29 Council Members) plus Canada, Japan, South Africa and the United States of America signed it.

It will enter into force once ratified by 5 States (perhaps in 2003?)

## Misgivings

Possible conflicts with existing national legislation

Non-signatory States where cybercriminals may act with impunity

Individual rights to privacy vs. extended surveillance powers granted to signatory countries

Possibility of personal data being transferred outside Europe to countries without comparable Data Protection legislation

Issuance of warrants seeking evidence and extradition