



President's Commission on Critical Infrastructure Protection

Briefing to the Advisory Committee

Progress Report

September 5, 1997



Overview

- **THE COMMISSION**
- **WHY INFRASTRUCTURE PROTECTION IS IMPORTANT**
- **VULNERABILITIES AND THREATS**
- **FINDINGS AND CONCLUSIONS**
- **SECTOR SUMMARIES**



Mission

Recommend a national policy for protecting and assuring
critical national infrastructures

- Determine vulnerabilities
- Identify threats — physical, cyber
- Develop policy & legislative issues
- Develop policy recommendations & implementation plan



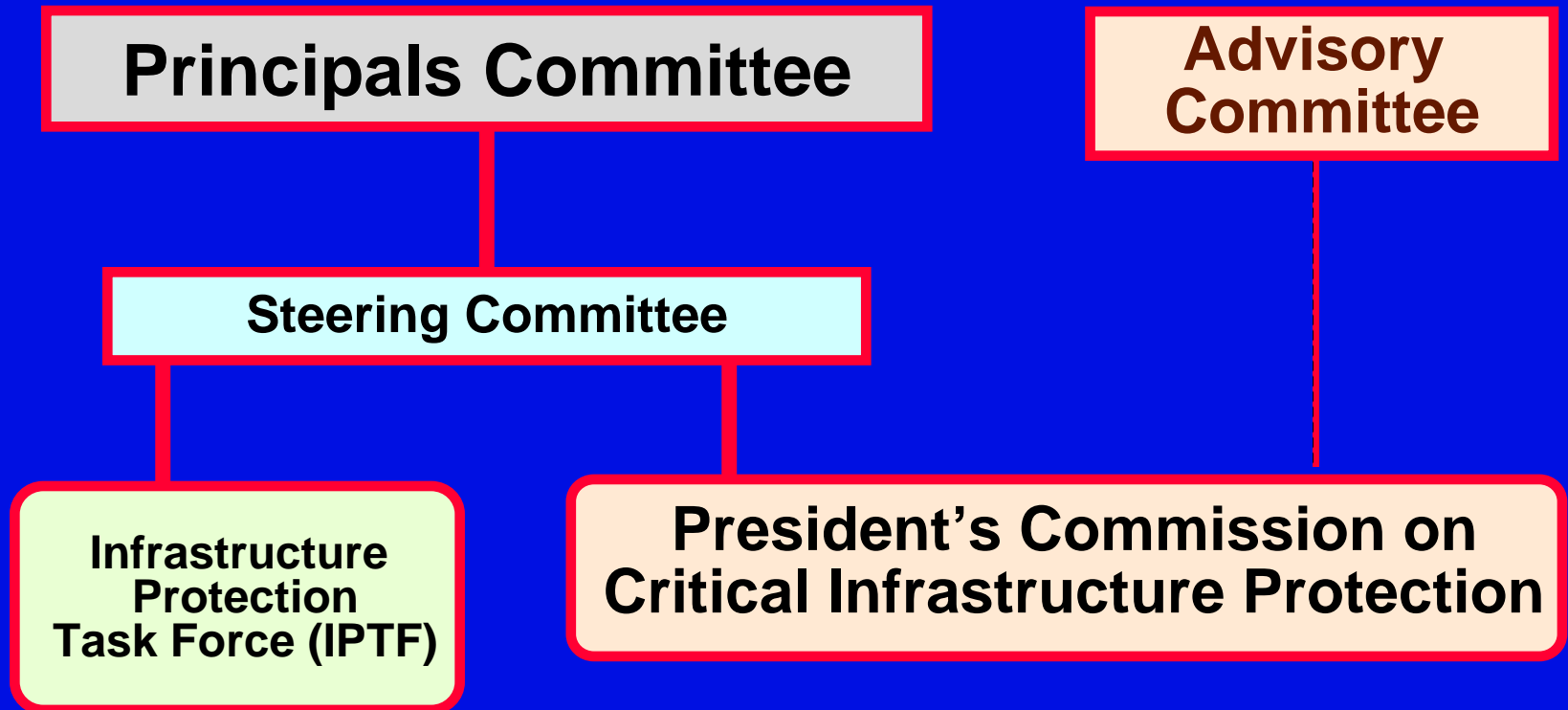
Critical Infrastructures

- Telecommunications
- Electric Power
- Transportation
- Oil & Gas
Delivery & Storage
- Banking & Finance
- Water
- Emergency Services
- Government Services

Why the Commission?

- Technology exists to severely degrade critical infrastructures
- Foreign governments, sub-national groups, even individuals have access to the tools and technology
- U.S. infrastructures are potential targets for full range of domestic and foreign threats
- Requirement is based on:
 - ▲ National Intelligence Estimate on Information Warfare
 - ▲ Presidential Decision Directive 39
 - ▲ Defense Science Board Studies
 - ▲ Critical Infrastructure Working Group (CIWG)

The Structure



Sector Teams

Information & Communications

Telecommunications
Computers & software
Internet
Satellites
Fiber Optics
...

Physical Distribution

Railroads
Highways
Air Traffic
Maritime
Intermodal
Pipelines
...

Energy

Electrical Power
Natural Gas
Petroleum
(Production,
Distribution, &
Storage)
...

Banking & Finance

Financial Transactions
Stock & Bond Markets
Federal Reserve
...
...

Vital Human Services

Water
Emergency Services
Government Services
...
...



Progress Report

- THE COMMISSION
- WHY INFRASTRUCTURE PROTECTION IS IMPORTANT
- VULNERABILITIES AND THREATS
- FINDINGS AND CONCLUSIONS
- SECTOR SUMMARIES

Imagine ...





What Do We Do?

- Who do you call?
- What do you need to know?
- How quickly?
- Why?
- Is it coincidence?
- Can you respond?

Why Infrastructures?

National Security

Reduce US ability to act in its own self interest

Public Confidence

Erode confidence in critical services

Economic Interest

Reduce American economic competitiveness

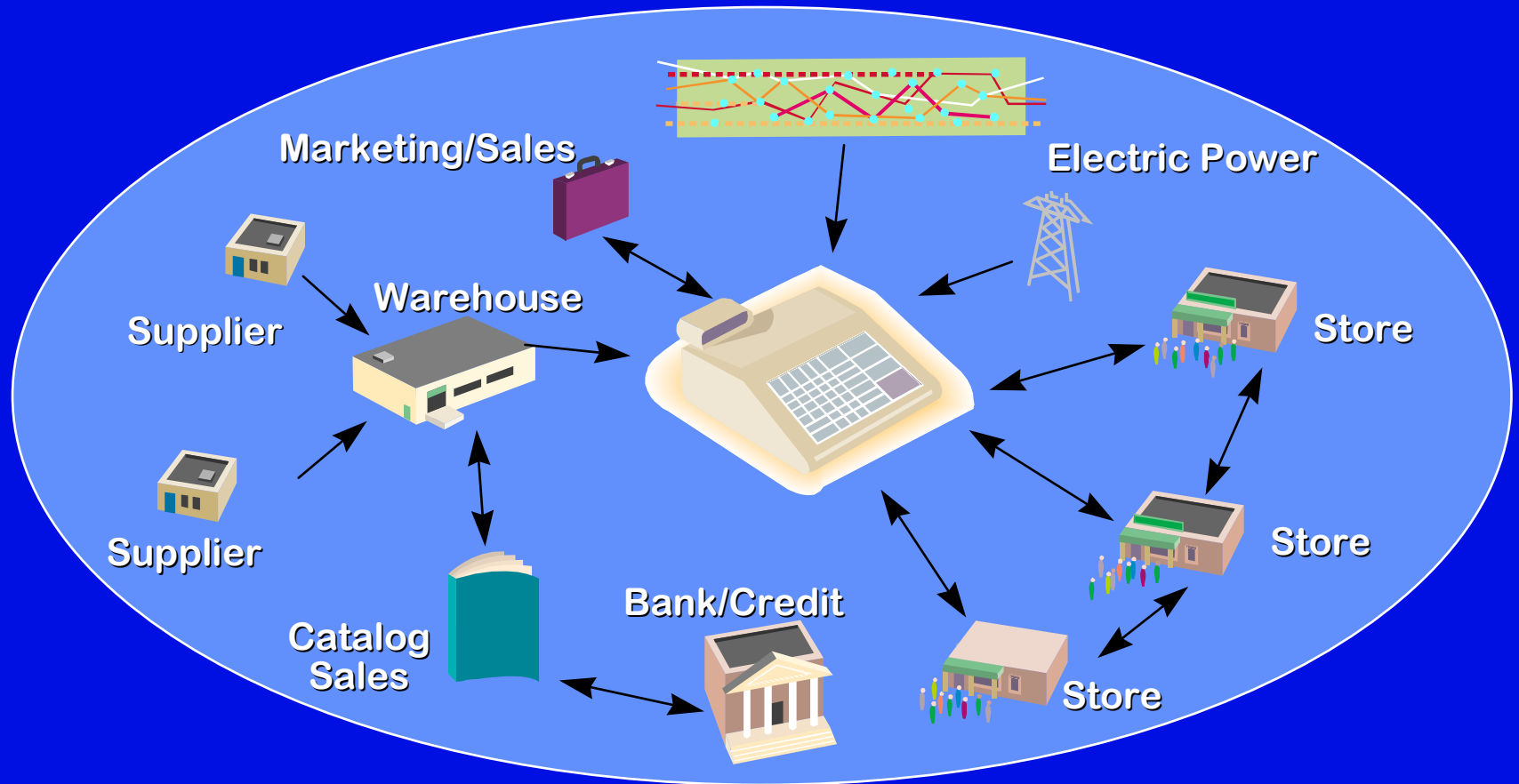


Critical Infrastructures

- High expectations and high confidence
- American dependence on the infrastructures
- Lynch-pin of conventional military power
- Key role in US global economic competitiveness
- Mutual interdependence
- Vulnerability to physical and cyber attack

Infrastructures are Attractive Targets

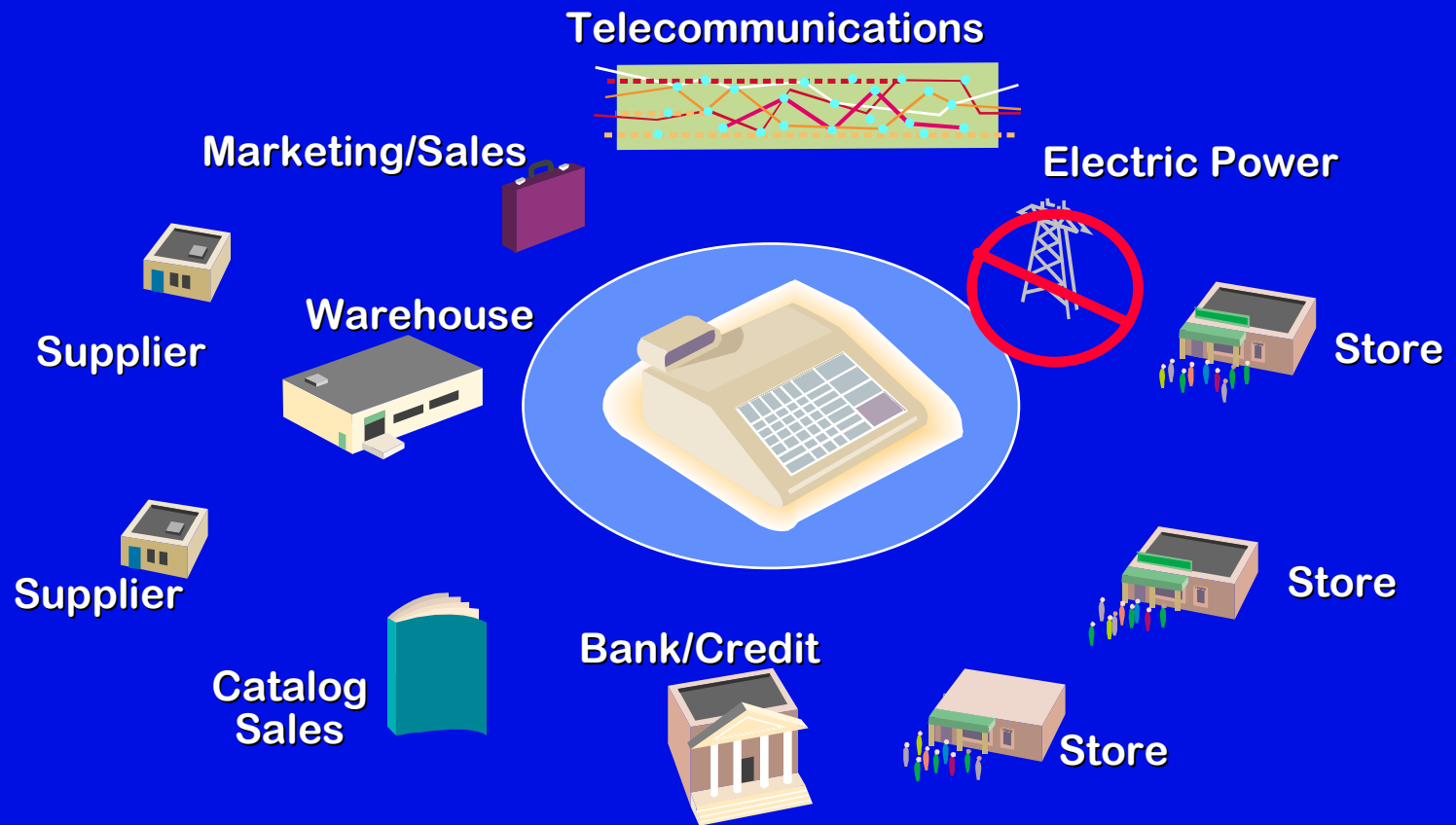
Infrastructure Delivers



Prosperity & Strength

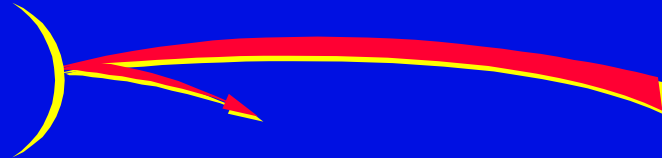
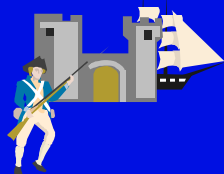


But ... New Risk

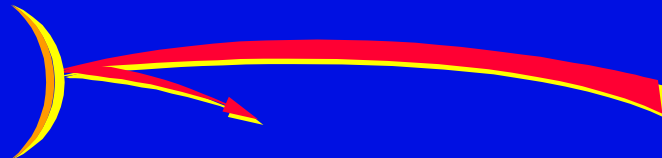
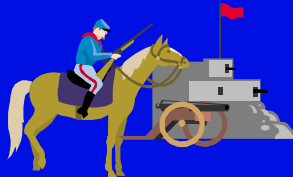


U.S. Infrastructures...

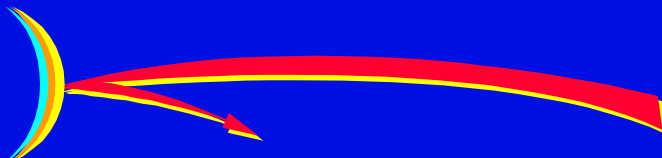
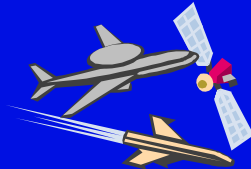
18th Century



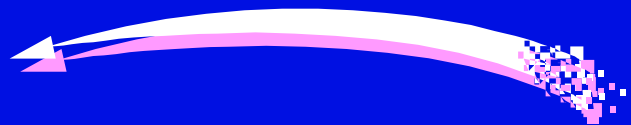
19th Century



20th Century



21st Century



**T
H
R
E
A
T**

... Always targets

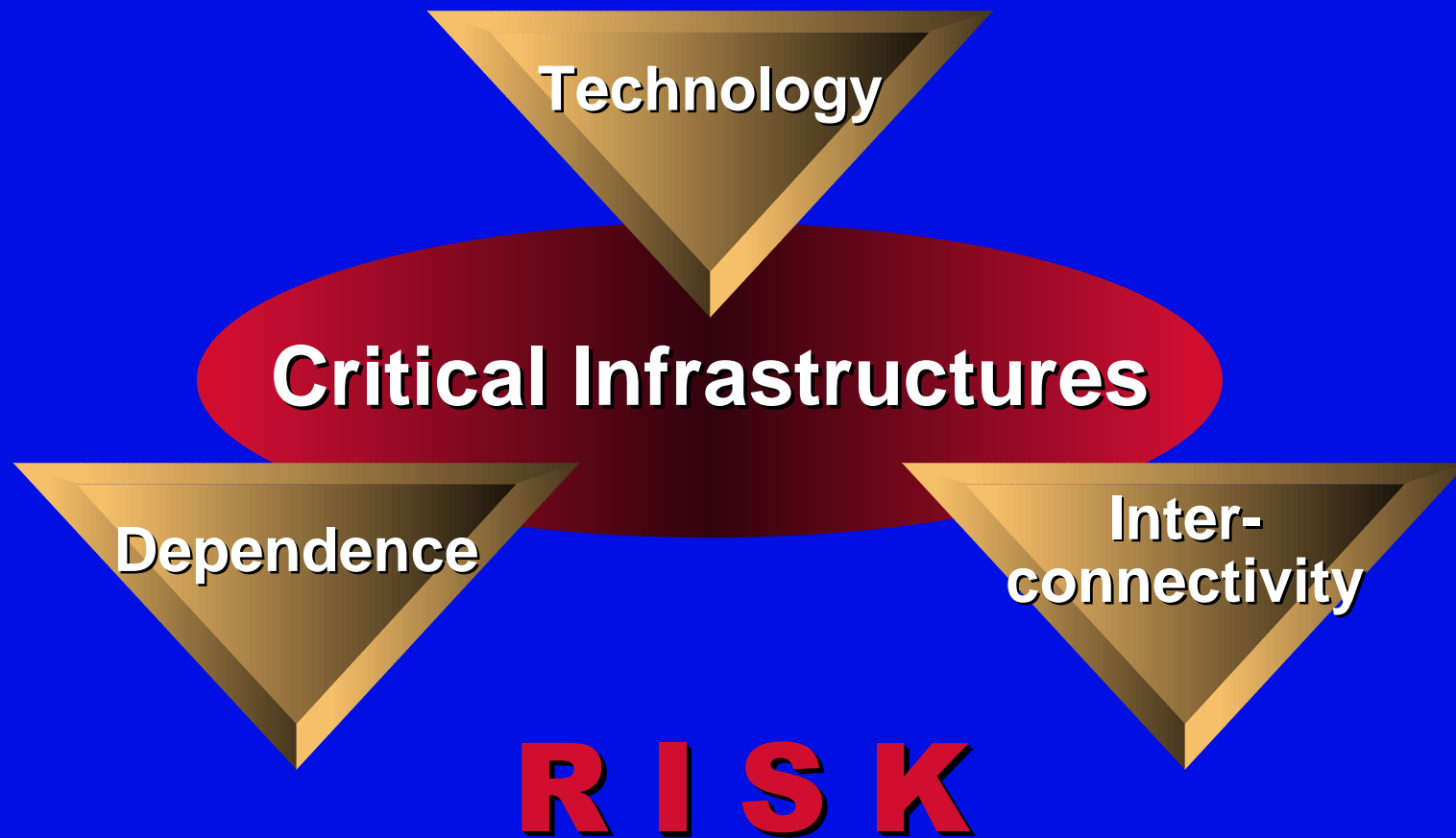




What Drives Our View

- **Technology**
- **Changing world**
- **Dependence on infrastructures**

Our View



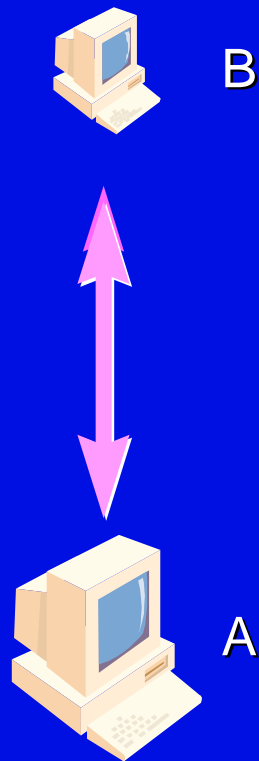


Advancing Technologies

- Standardized general purpose hardware
- Ubiquitous operating systems
- Open architectures
- Software
- Evolving megacenters
- Heightened intrusion proficiency

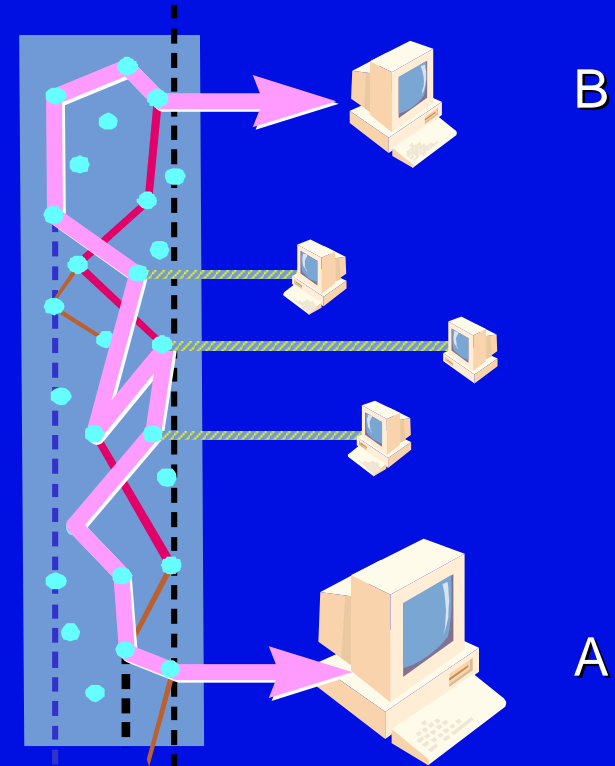
Tremendous Capability: New Risk

Increasing Exposure



How we *think* we communicate

The Internet



How we *really* communicate



The World Has Changed

Information ▶ **Property & Commodity**

Global Networks ▶ **Dual-edge Swords**

Globalization ▶ **World-wide Players**

Cyber Dimension ▶ **No Boundaries**

Deregulation/Restructuring ▶ **Potential Vulnerabilities**

Military Superiority ▶ **New Competition**

Pace of Change ▶ **?**



New Risks

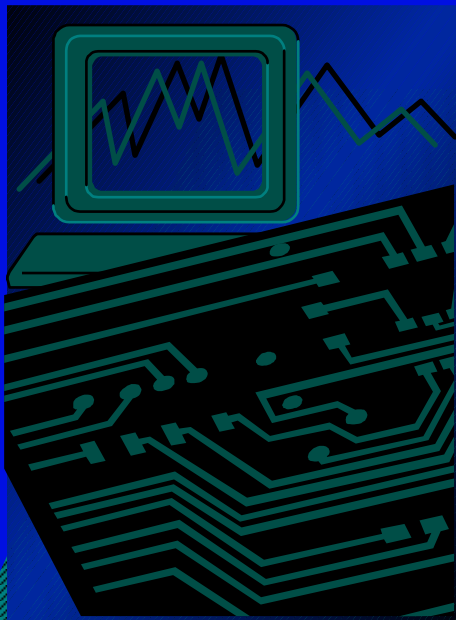
- Tools to do harm are widely available
- Vulnerability information is easily accessible
- Insiders represent increased risk
- Interdependencies of systems make attack consequences more severe
- Globalization of infrastructures increases exposure to potential harm
- Restructuring and competition may decrease assurance



Progress Report

- THE COMMISSION
- WHY INFRASTRUCTURE PROTECTION IS IMPORTANT
- VULNERABILITIES AND THREATS
- FINDINGS AND CONCLUSIONS
- SECTOR SUMMARIES

Threat....



Perspective on Threat

- New understanding of threat
- Actor and intent: unknown
- Capability to do harm: expansive & growing
 - ▲ Skills
 - ▲ Technology
- No shortage of opportunity

Vulnerabilities: *A New Dimension*



COMPLEXITIES

RESTRUCTURING



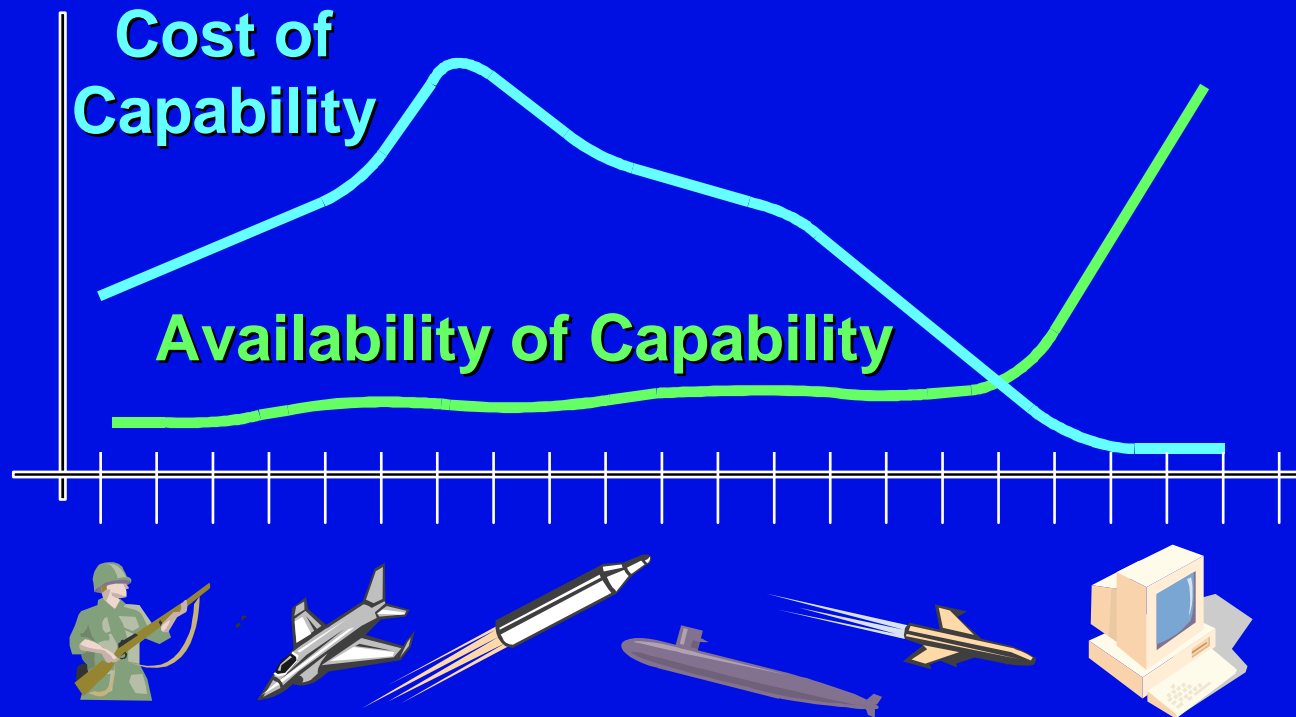
INTERDEPENDENCIES

Vulnerabilities:

A New Dimension

- Physical vulnerabilities and threats are known
- Cyber vulnerabilities are growing but are not well understood
- There is less appreciation for interdependencies and complexity

Evolution of Threat



Threat Profile

Known Threat



Limited capability +
marginal opportunity =
High Risk of detection

Emerging Threat

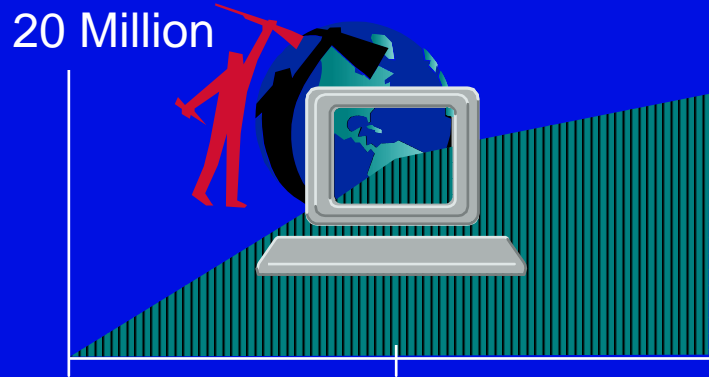


Widening capability +
broad opportunity =
Low Risk of detection



Increasing Risk

Availability of Skills



Growing Opportunity



2,000



Internet Incidents



A New Arsenal

WWW facilitates physical attacks

Denial of Service

Data Theft

Data Modification

Resource Abuse



Intrusions

Web Assaults

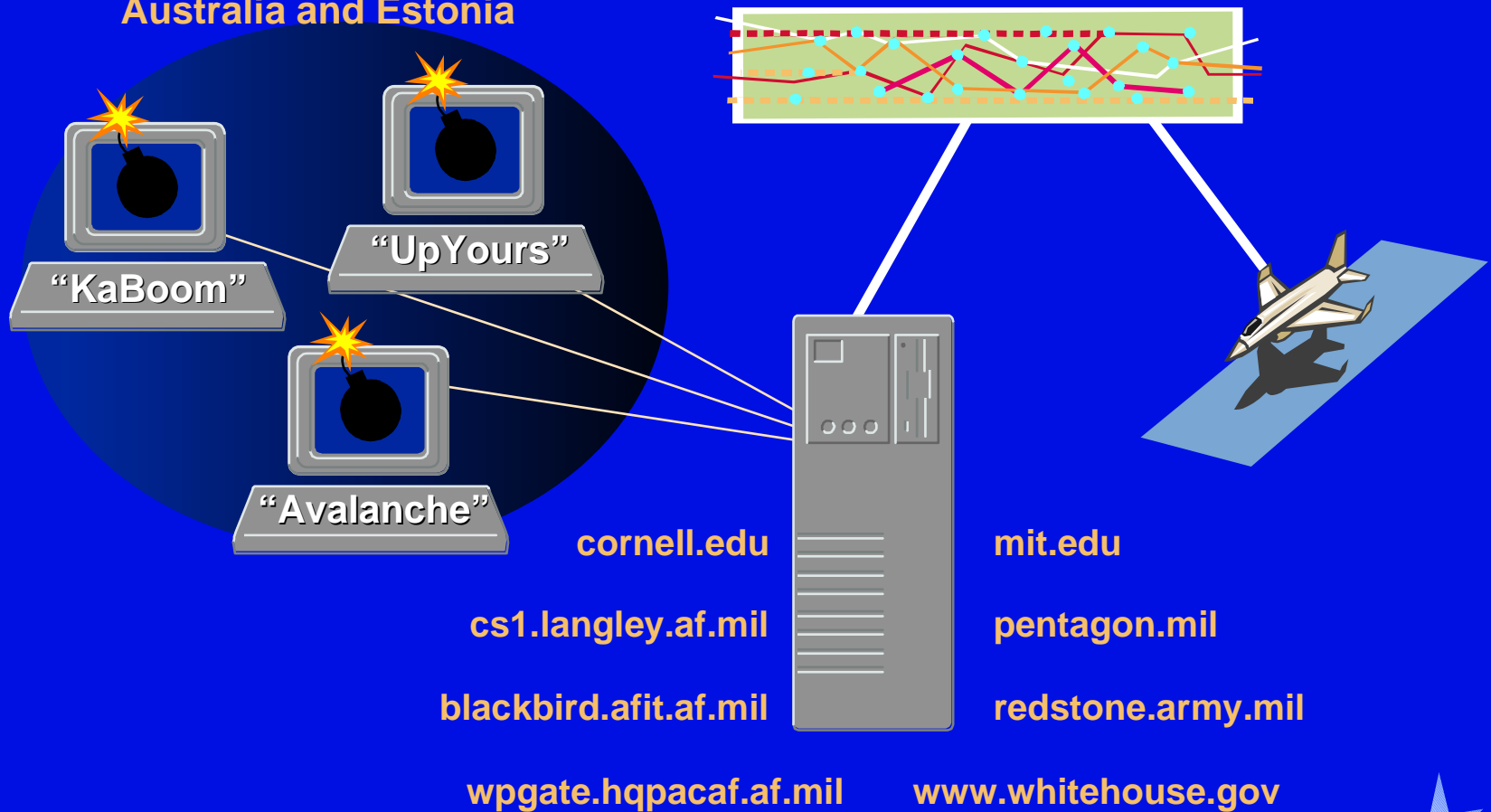
Viruses

E-Mail Attacks



E-mail Flooding

Australia and Estonia



Intrusion





Potential for Damage:

Other Incidents

■ Targeting

- ▲ Penetrate computers for targeting information

■ Loss of Service

- ▲ Internet Service Providers
- ▲ 911
- ▲ Emergency Alerting System

■ Theft

- ▲ Credit Cards
- ▲ Counterfeiting
- ▲ Intellectual Property
- ▲ Proprietary Data

Threat Spectrum

National Security Threats	Info Warrior	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	Institutional Hacker	Monetary Gain Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

**I
N
S
I
D
E
R
S**

Imagine you're in charge?

The case for an analytic capability





Progress Report

- THE COMMISSION
- WHY INFRASTRUCTURE PROTECTION IS IMPORTANT
- VULNERABILITIES AND THREATS
- **FINDINGS AND CONCLUSIONS**
- SECTOR SUMMARIES

Findings

- Capability for harm is real and widespread
- Vulnerabilities are serious and increasing
- Protection-related information must be shared
- Warning capability for cyber attacks must be developed
- Nation-wide analytic capability is needed for infrastructure protection

Findings

- Government must prepare to deal with cyber-threat
- Owners and operators must be informed to protect from this range of threat



Findings

- Technology is needed for detection, identification, and defense against cyber-threats
- Investment is needed in defensive tools



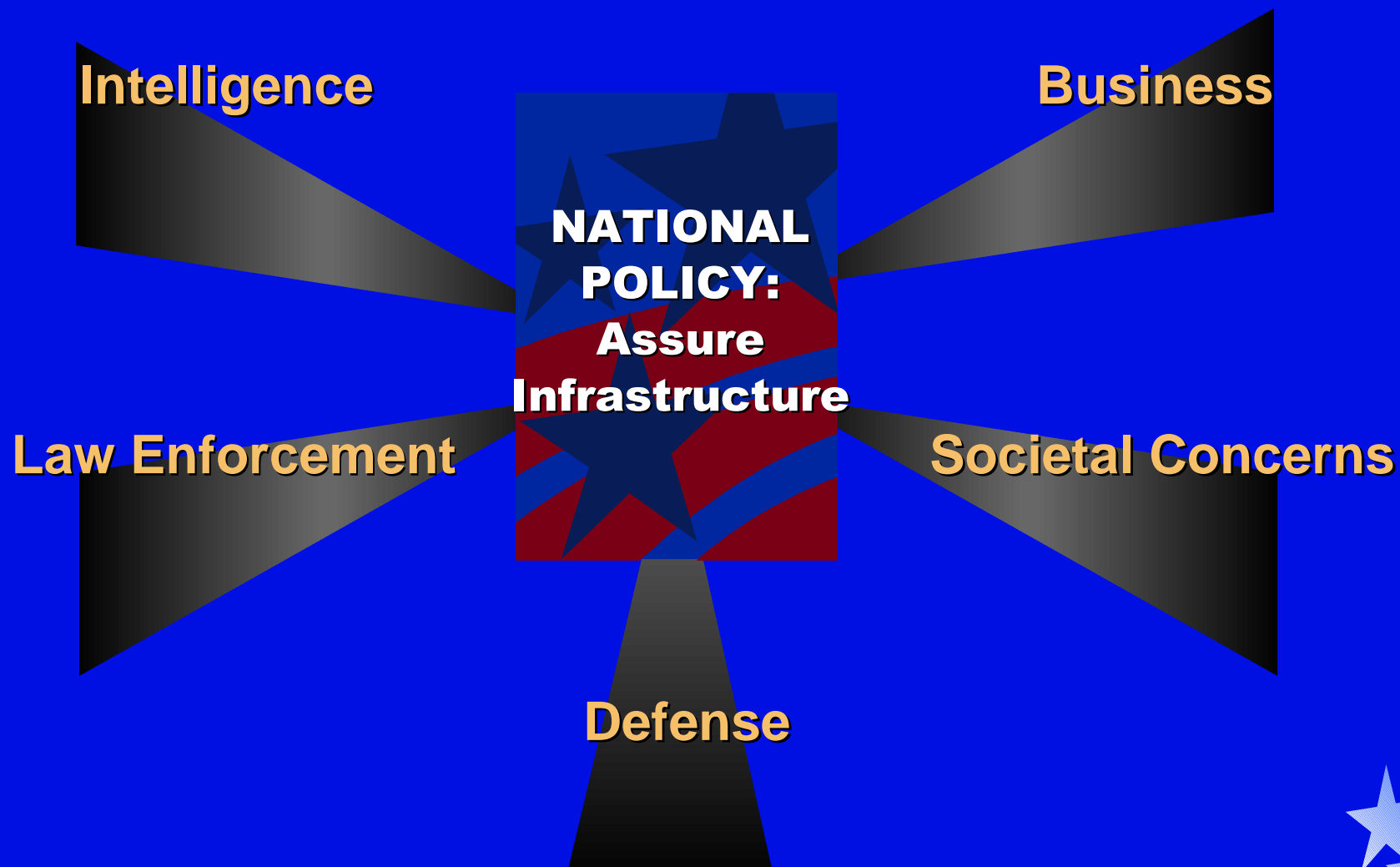
Conclusions

- National risk is growing with increasing reliance on information & communications infrastructure
- Public confidence is critical
- Risk is shared among public & private interests

**Partnership is the Foundation for
Infrastructure Assurance**

Infrastructure Protection

Common Purpose: Diverse Interests





Progress Report

- THE COMMISSION
- WHY INFRASTRUCTURE PROTECTION IS IMPORTANT
- VULNERABILITIES AND THREATS
- FINDINGS AND CONCLUSIONS
- SECTOR SUMMARIES