AFCEA Atlanta

Information Security & Information Warfare :

August 22, 1996

Dr. Myron L. Cramer
Georgia Tech Research Institute
400 Tenth Street
Atlanta, Georgia 30332-0840
(404) 894-7292
myron.cramer@gtri.gatech.edu

Georgia Tech Research Institute

TOPICS

- Describe Information Warfare (IW).
- Discuss different perspectives for IW.

- Describe issues for Information Security.

THE INFORMATION AGE

Civilization:

Principal Activity:

farming	manufacturing	services

Empowering Wealth:

labor, land	labor, materials	knowledge, info systems

Examples:

fiefdoms, plantations, …	automobiles, electric motors, steel, …	software, marketing, information services, …

Georgia Tech Research Institute

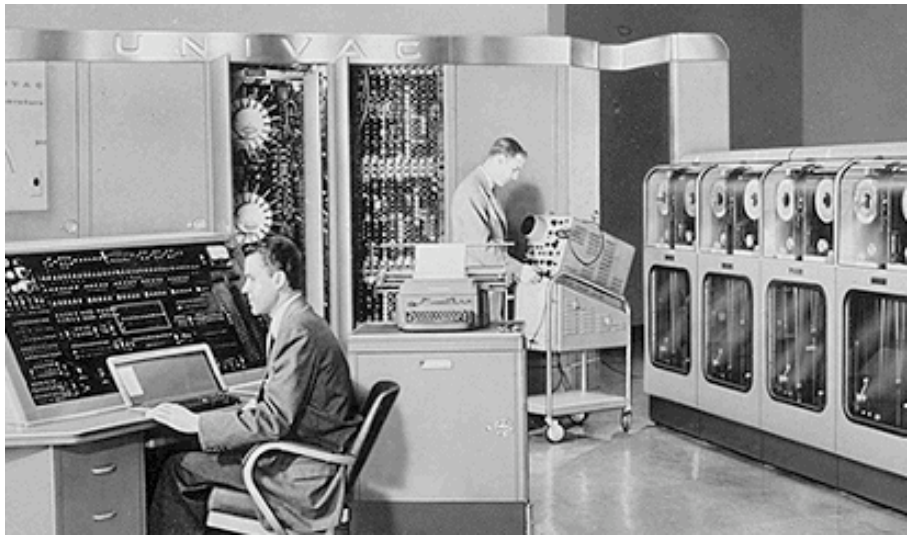
CONSEQUENCES ...

Information Warfare is a consequence of the Information Revolution.

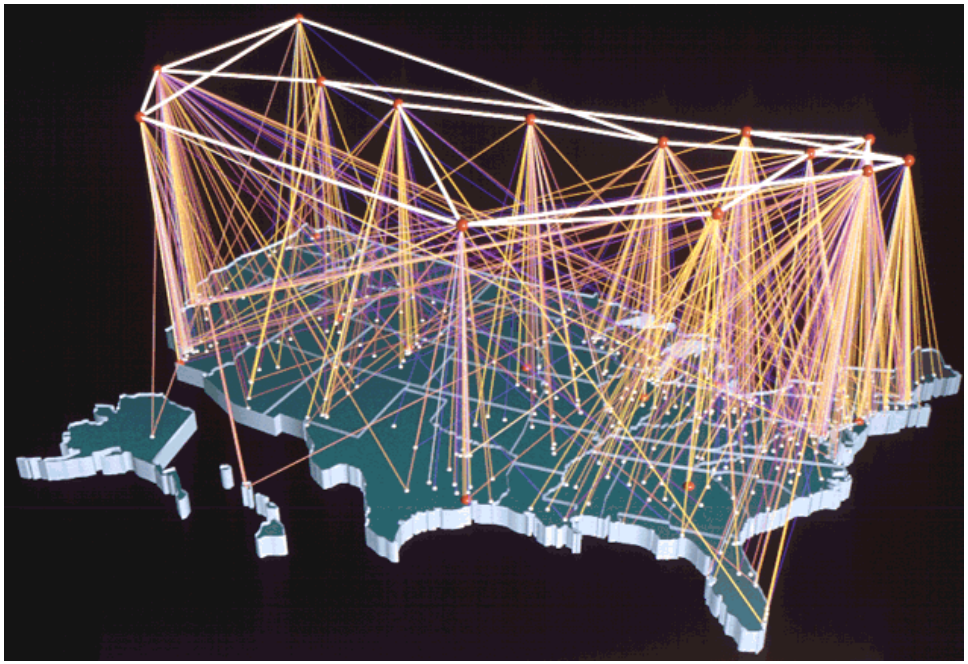
- Information carries more value than previously
- Competitive advantages can impact an organization's success or failure

Assertion:

» It is important to understand the framework created by the new information technologies and new paradigms.



THE NATURE OF COMMUNICATIONS HAS CHANGED



- Transition from voice to digital data
- Growth of Communication Networks
- Entry of computers into government and business
- Wide-spread use of advanced commercial technologies, standards, and products

MILITARY CONTEXT

- Dissemination of intelligence
- Control of air and maneuver forces
- Control of direct and indirect fire systems
- Operation of air defense
- Distribution of materiel and support resources

THE NEW INFORMATION TECHNOLOGIES

The New Information Technologies:

Computer-Aided Design	**Fax Machines**
Paperless Manufacturing	**Scanners**
Groupware	**Pen Notebooks**
Online Services	**Flash Technology**
Document Management	**Advanced Fiber Optics**
Customer Service Technology	**Wireless Technology**
Point-Of-Sale Terminals	**Videoconferencing**
Servers	**Graphics Technology**
Networks	**Data Compression**
Databases	**Object Orientation**
Printers	**Virtual Reality**
Voice Recognition	**Geographic Systems**
Storage Protection	

U.S. News & World Report, May 2, 1994

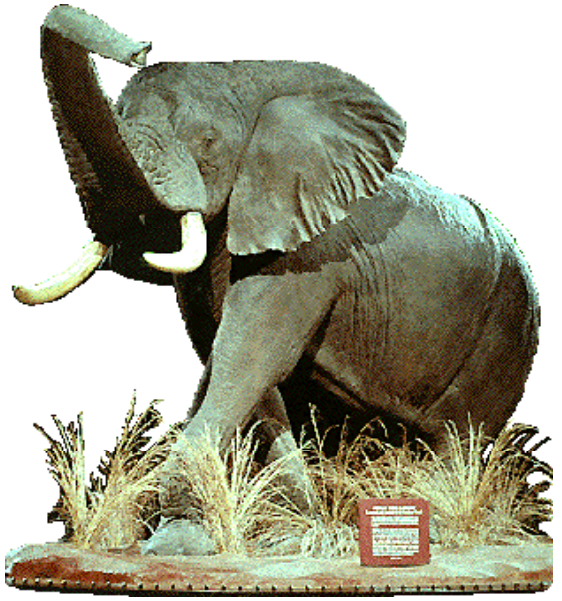
- are only technologies,
- of themselves are neither good nor bad,
- can be used for great benefit, or,
- can lead to disaster.

The trick is to be able to know the difference.

Georgia Tech Research Institute

DEFINITION ...

Information Warfare includes:



» ways of gaining and maintaining an **information advantage** over competitors or adversaries.

» The term **Dominant Battlespace Knowledge** is currently used to convey the desired result of successful IW practices. Although IW is a general term including a wide variety of different concepts, it is usually connotes a primarily strategic focus. Command and Control Warfare (C2W) is defined as the combat use of IW.

INFORMATION WARFARE DOCTRINE

Information Warfare is a declared priority doctrine.

- The importance to our national interests of modern information systems and their contents has been has been acknowledged and declared a national priority by the President and by the JCS.
- The Defense Department has acknowledged the increasing value of information and information systems and in *DoD Instruction TS-3600.1* has assigned formal responsibilities.
- The Joint Chiefs of Staff have issued *Memorandum of Policy (MOP) 30* defining *Command & Control Warfare* as the military element of *Information Warfare*.

Georgia Tech Research Institute

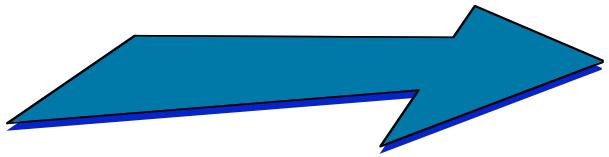
MILITARY BACKGROUND: DESERT STORM

The origins of Information Warfare doctrine:

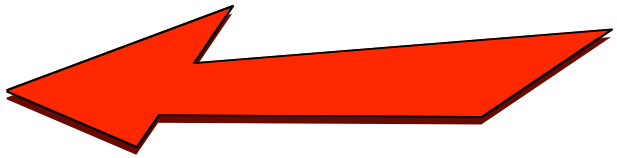
- defined by General Schwartzkopf
- born of the necessity to integrate several previously separate disciplines

COMMAND & CONTROL WARFARE DEFINED

C2W is the military component of Information Warfare:



- **Protecting** our information systems



- **Countering** an adversary's information systems

*It is defined as the **integrated use** of:*

- » Operations Security (OPSEC)
- » Psychological Operations (PSYOP)
- » Military Deception
- » Electronic Warfare (EW)
- » Physical Destruction

*mutually supported by **intelligence** to:*

- » deny information to
- » influence
- » degrade or destroy adversary C2 capabilities
- » while protecting friendly C2 capabilities against such actions

Georgia Tech Research Institute

CYBERWAR

PSYCHOLOGICAL OPERATIONS

The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

» Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups, and individuals.

» Methods of PSYOP include:
- Pamphlet distribution
- Commando Solo broadcasts (radio, television)
- Loudspeakers

OPERATIONS SECURITY (OPSEC)

OPSEC is the key to denial of information.

» A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

» OPSEC methods include:

- Camouflage
- Night Operations to operationally minimize visibility to enemy sensors
- Information security (INFOSEC)
- OPSEC monitoring

MILITARY DECEPTION

Actions executed to mislead foreign decision makers

» causing them to derive and accept the intended view of military capabilities, intentions, operations, or other activities

» Methods of conducting deception include:

Drones	The use of drones to simulate air missions to draw attention from the real strikes
Decoys	Placement of fake military equipment for observation by enemy sensors
Feints	Military operation intended primarily to draw enemy forces
Ground Forces	Use of ground forces to be observed by enemy sensors
Special Forces	Use of special forces to create deceptions
Fictitious Radio	Use of fictitious radio traffic to deceive the enemy

Georgia Tech Research Institute

ROLE OF NEWS MEDIA

The importance of the news coverage was recognized by all participants.

Georgia Tech Research Institute

SOME USED THIS SKILLFULLY …

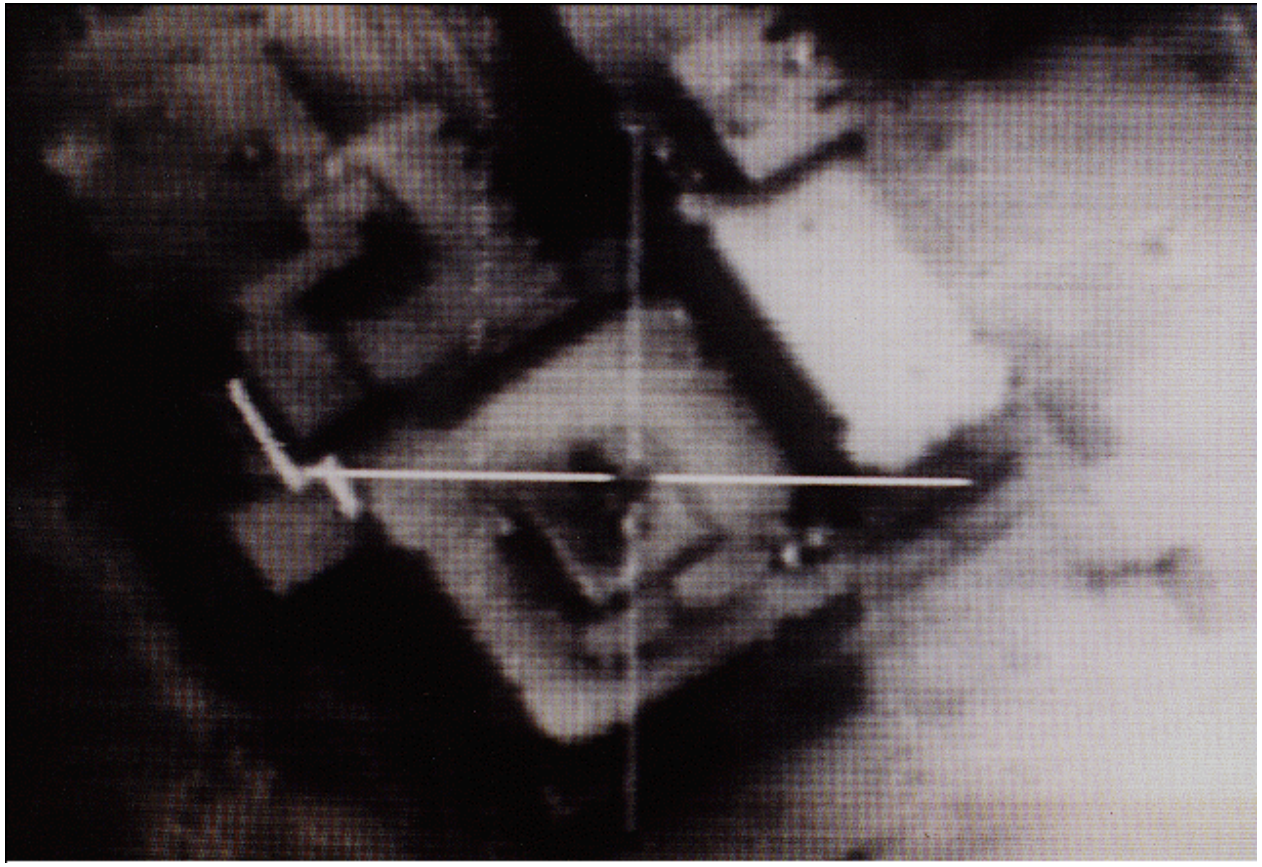
Georgia Tech Research Institute

AND SOME DID NOT ...

Georgia Tech Research Institute

COMMAND & CONTROL DESTRUCTION

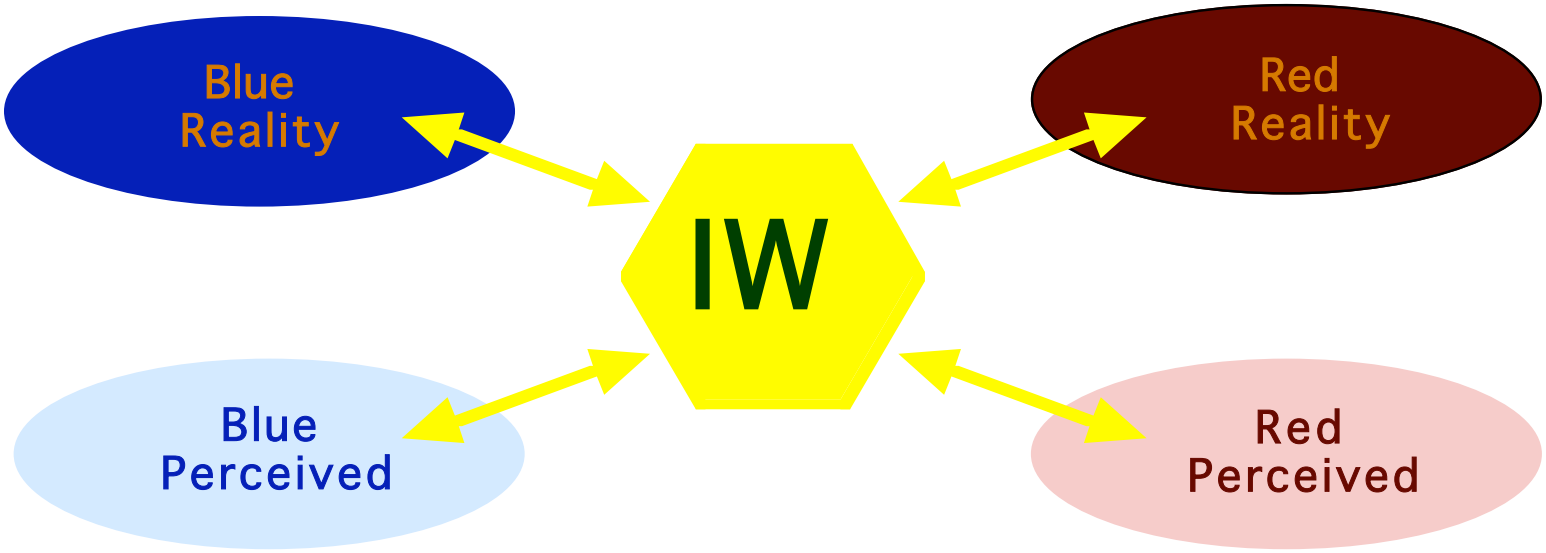
The precision of modern weapons utilized new targeting capabilities.



View from F-117 Bomb Camera

NON-LINEARITY OF IW/C2W

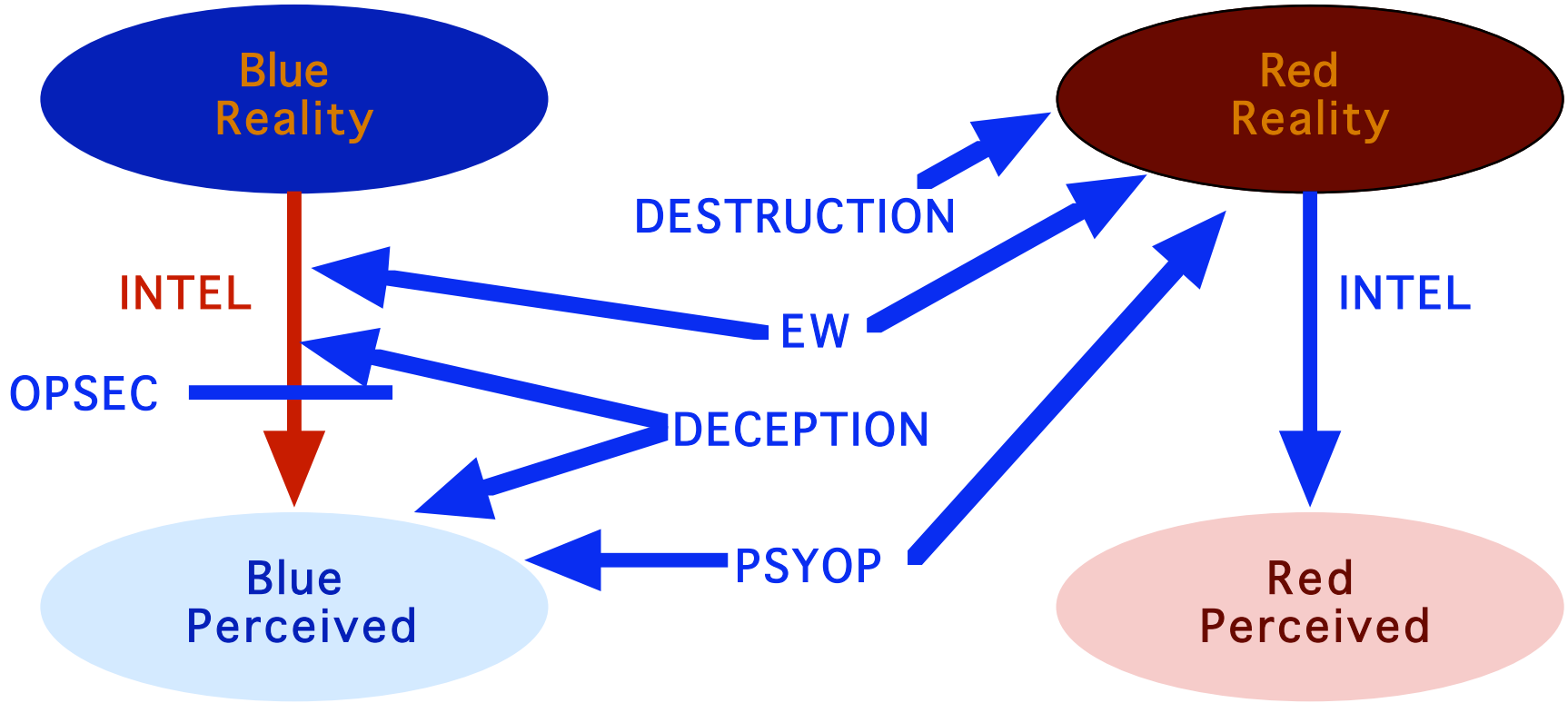
It is important to capture the non-linearity involved in seeing what you are looking for.



This effect is important in the elements of C2W.

INTEGRATED USE OF IW/C2W

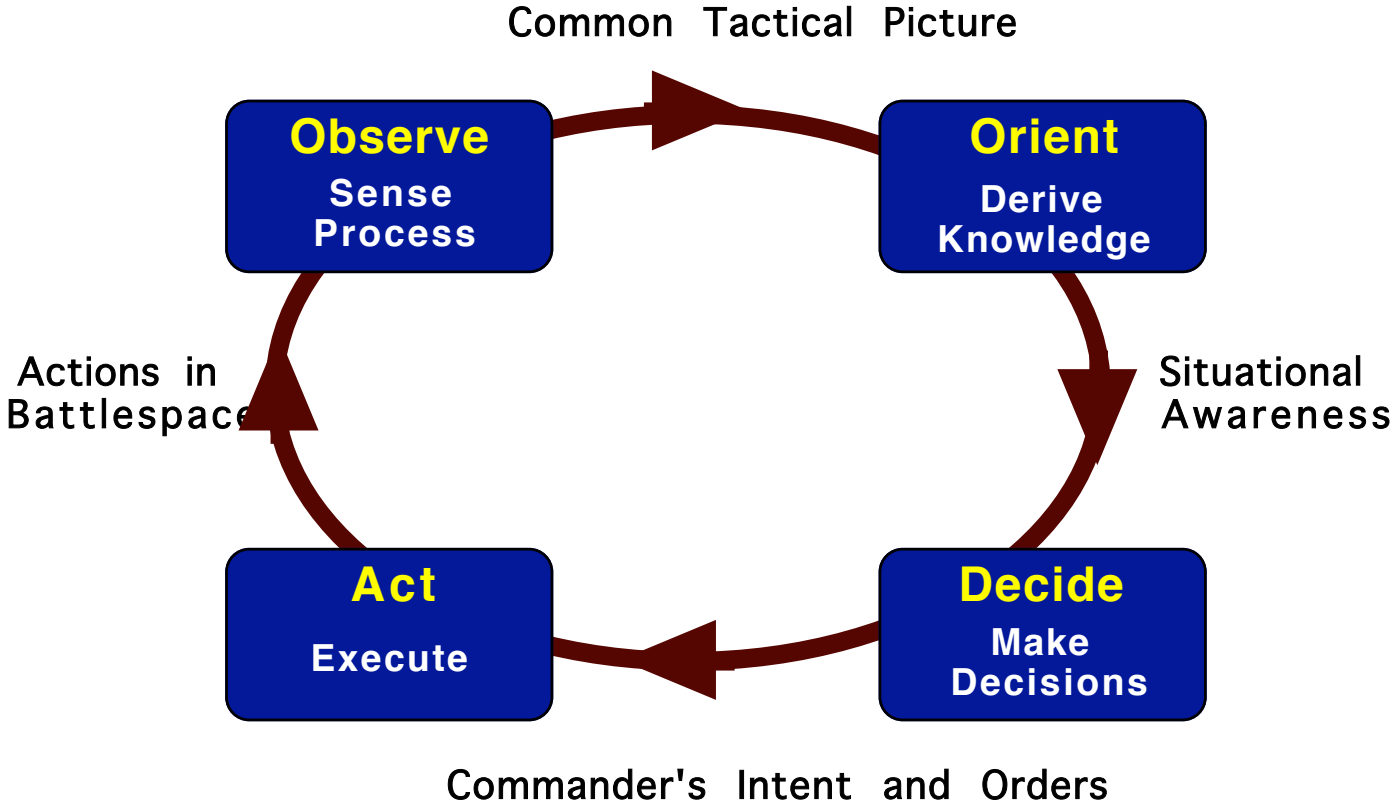
The use of the IW elements is highly interdependent



Georgia Tech Research Institute

COMMAND AND CONTROL PROCESS

The functional control activities represented in a Command and Control process are represented by the Observe-Orient-Decide-Act (OODA) Loop.



Georgia Tech Research Institute

COMMERCIAL RELEVANCE

Problem with Military Terminology:

- Although the origins of Information Warfare concepts are military, the commercial applications may be much more significant.
- The problem in making the translation is the military terminology that may not be directly applicable to business.

Conclusion:

» There is a need for a less restrictive decomposition of Information Warfare that is more directly applicable to business.

COMMERCIAL PERSPECTIVE

New information systems exert a powerful market force to allow competitive advantages:

"Information technology is a strategic weapon." –Staser Holcomb, USAA

- USAA has become the country's fifth-largest car insurer by use of information technologies such as toll-free lines, reduction in use of paper documents, use of laptop computers and cellular phones by adjusters.
- K-Mart's information systems begin with bar-code scanners, LANs, private satellite links to corporate headquarters, allowing management to view evolving sales data.
- American Airlines SABRE reservation system allows flight to be efficiently scheduled and correlated with crews, food, and other related items. Flights can be rescheduled as needed with all impacted items managed.
- Boeing's new 777 was designed as the first paperless plane. CAD/CAM systems are so precise that the aircraft parts fit so well that the plane lacks the ripples common in the past.

FROM AN INFORMATION SYSTEM PERSPECTIVE...

Information Warfare includes:

- **Collection** (information entry points, sensors)
- **Protection** (security, encryption)
- **Denial** (denial of information to an adversary, manipulation or compromise of his information sources)
- **Management** (information control, data storage, access, processing)
- **Transport** (data communication, dissemination, switching)

COLLECTION

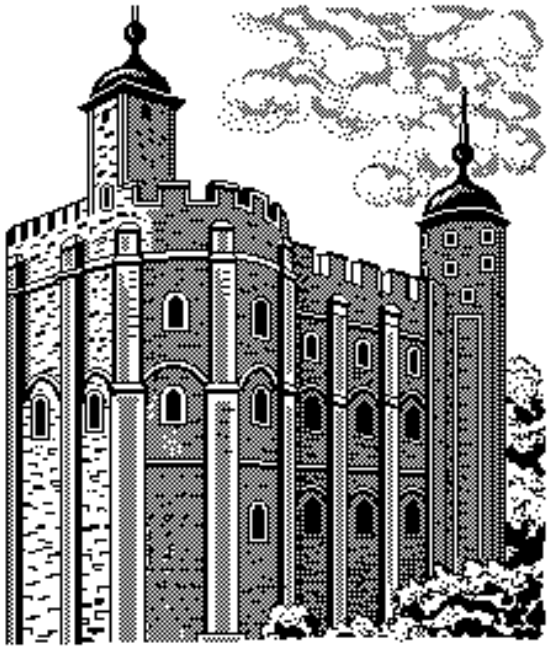
Collection includes the mechanisms by which information enters an organization's systems:

- Information includes data to support operations:
  - » planning, executing, monitoring, and reporting
- Information issues:
  - » quantity (completeness), quality (accuracy), and timeliness.
- Business examples:
  - » point-of-sale, market surveys, government statistics, internal management data, competitive intelligence

PROTECTION

Some information may have high value to a competitor:

- **proprietary**: future plans, product technical data, customer lists, personnel files, and financial records
- **non-proprietary:** travel schedules, phone directories, organization charts



Protection includes measures and assurances against:

- **Compromise** of data and information to a competitor
- **Destruction**, corruption or loss of service, information system attacks, loss of confidence

DENIAL

Denial includes measures beyond normal protection to compromise or counter a competitor's information systems:

- **Direct Attacks:** although risky and illegal, they may be used by a desperate adversary
- **Misinformation:** providing false data for an adversary's information systems

Denial Objectives:

- **Delay**
- **Destroy**
- **Disrupt**
- **Deceive**

Georgia Tech Research Institute

MANAGEMENT

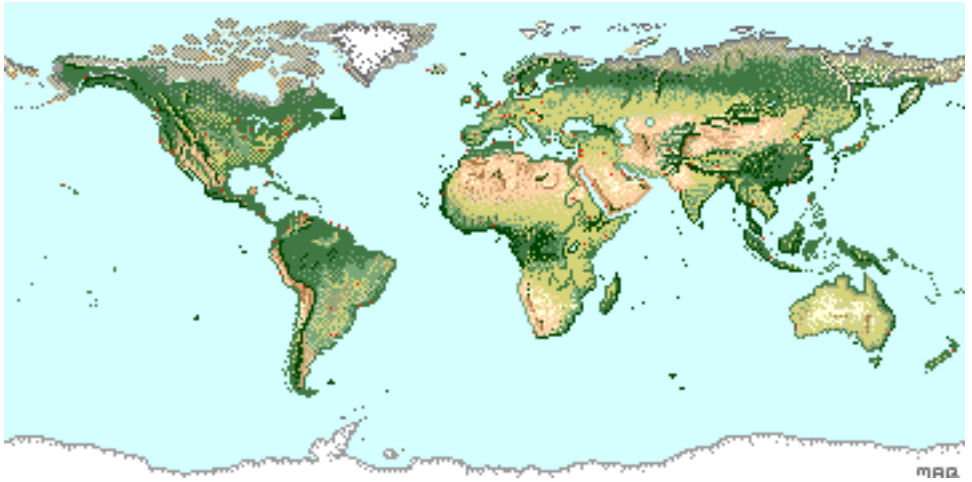
The life-cycle control of information in a distributed, decentralized, networked computing environment.

- Issues for corporate data managers:
  - » Where is the data?
  - » Who has it?
  - » Which version is the most current?
  - » Which data to keep or destroy?
  - » How to store archival data for future computer generations?
- Intellectual property issues:
  - » Where is it?
  - » How is it protected?
  - » Where are paper records needed?

TRANSPORT

Moving data from collection to storage to users.

- Issues are speed, reliability, and controllability.
- Speed affects the timeliness of the information and its impact on an organization's operations including the ability to respond to changing situations.



- Reliability affects the degree to which information can be depended upon in day-to-day operations.
- Controllability describes the ability of decision makers to direct information to users as needed.

PROTECTION ISSUES

Protecting friendly C2 includes the following issues:

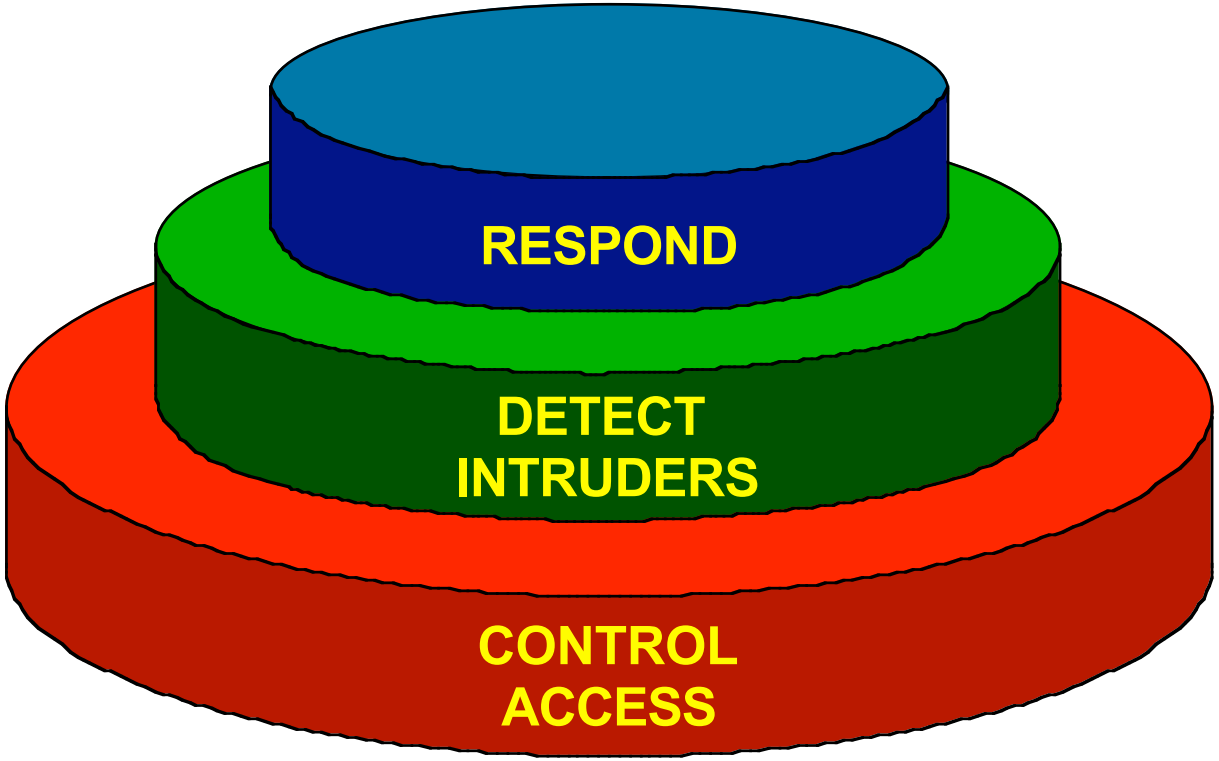
Authentication:	validation of transmissions, messages, and users
Confidentiality:	assurance that information is not disclosed to unauthorized entitites
Integrity:	assurance that data or processes have not been altered or corrupted by chance or by malice
Reliability & Availability:	assurance that information systems will work when called upon

MEASURES OF EFFECTIVENESS

	Quantity	Time	Quality
Authentication	Number of invalid users accepted Number of valid users rejected	Mean time to compromise	User confidence
Confidentiality	Number of invalid accesses achieved	Mean time to access	User confidence
Integrity	Error rates	Mean time to corrupt	User confidence
Reliability & Availability	System reliability R(t) Percent of time available	Mean time to disrupt	User confidence

ROLE OF INTRUSION DETECTION

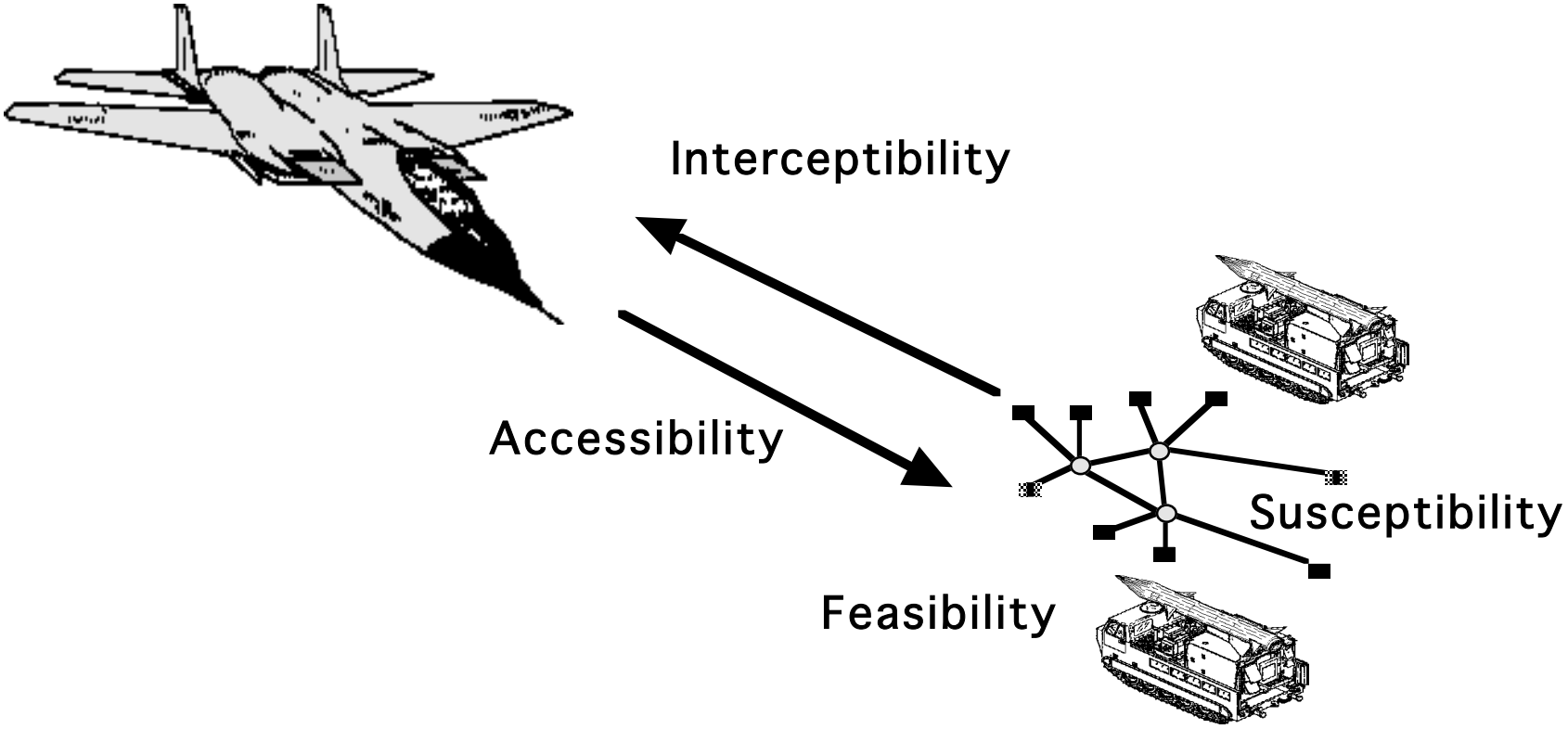
Intrusion detection systems are the second layer of protection.



Georgia Tech Research Institute

EW PERSPECTIVE

The Classic EW Vulnerability Analysis includes four elements:

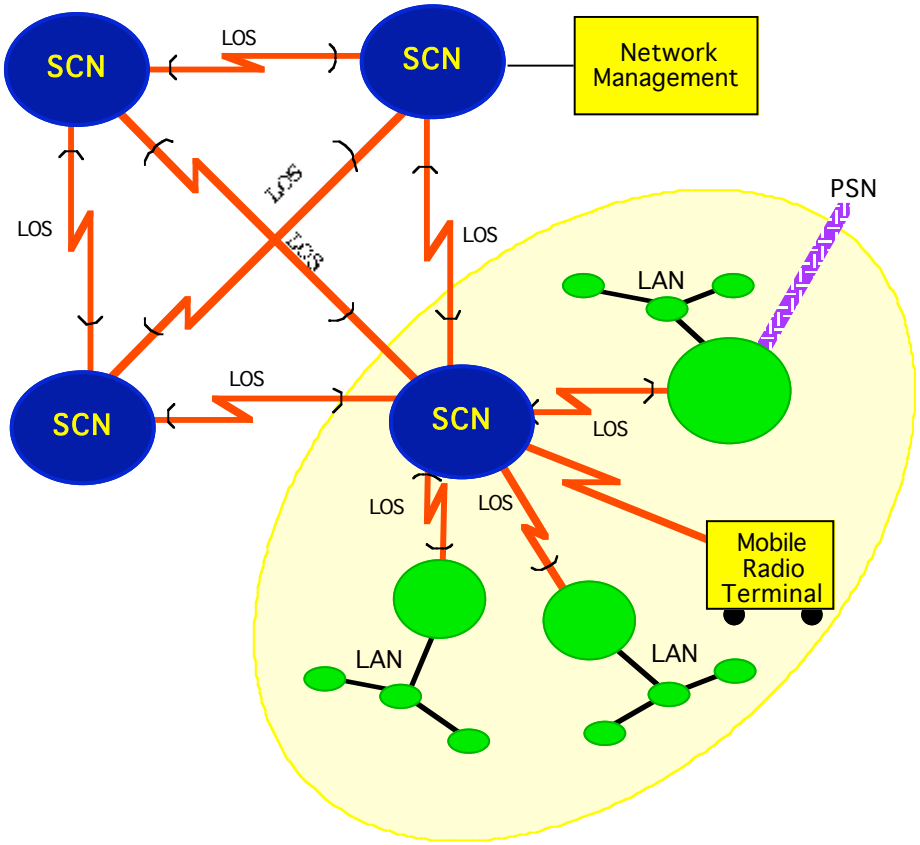


These elements can be applied to modeling C2W attack on tactical data links.

Georgia Tech Research Institute

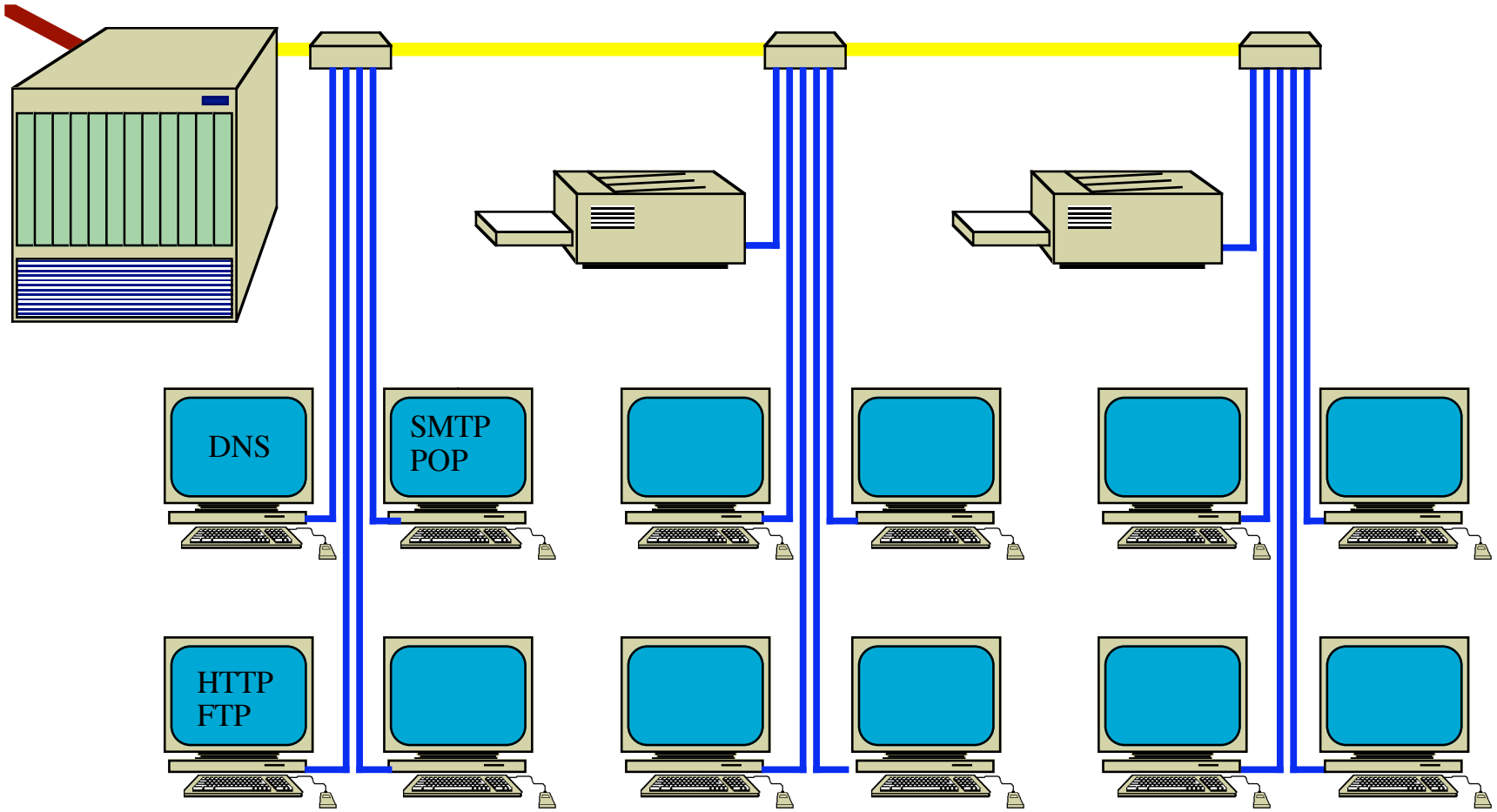
NETWORK TEMPLATES

Network Templates provide Electronic Signatures of Network elements.



Georgia Tech Research Institute

"COMPUTER" ORDER OF BATTLE



Georgia Tech Research Institute

INTERCEPTIBILITY MODEL

Interceptibility includes factors for technical and operational intelligence.

- Technical intelligence:
  - » How well do we know the system designs and protocols?
- Operational intelligence:
  - » Can we detect, locate, identify, and characterize operational users in the target net?

ACCESSIBILITY MODEL

Accessibility includes factors for link, transport, and functional penetration.

- Link:
  - » How well can I enter the links?
- Transport:
  - » How well can this link transport my data?
- Functional:
  - » What functional penetration is achieved

GAME THEORY ELEMENT

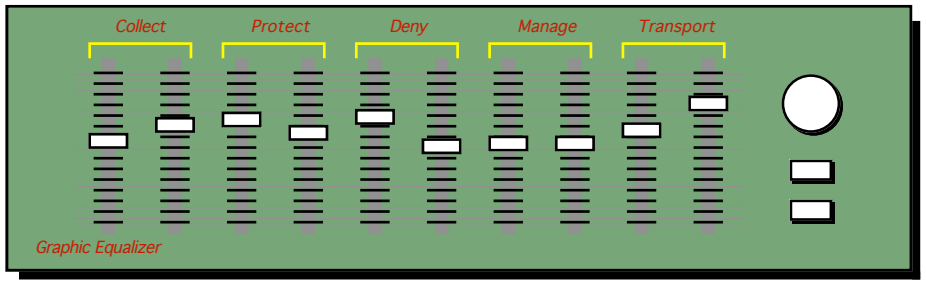
In a competitive environment, the optimum strategy may depend on what the competition is doing.

- In this example, Options 1, 2, and 3 are progressively more expensive in terms of capital investment in information system technologies.
- Each option provides a relative market share benefit over a competitor investing less.

		Player A		
	Benefit/ Cost	Option 1	Option 2	Option 3
Player B	Option 1	0	High	Low
	Option 2	High	0	High
	Option 3	Low	High	0

SEEKING THE RIGHT BALANCE…

The same considerations are true for each of the elements of Collection, Protection, Denial, Management, and Transport.



- The trick is to find the right balance among these.
- Factors include market opportunities, likely competitor actions, and current competitive situation.

Georgia Tech Research Institute

SUMMARY

This presentation:

- Described Information Warfare (IW).
- Discussed different perspectives for IW.
- Described issues for Information Security.