# Your Information Security Silver Bullet

# United States Strategic Command

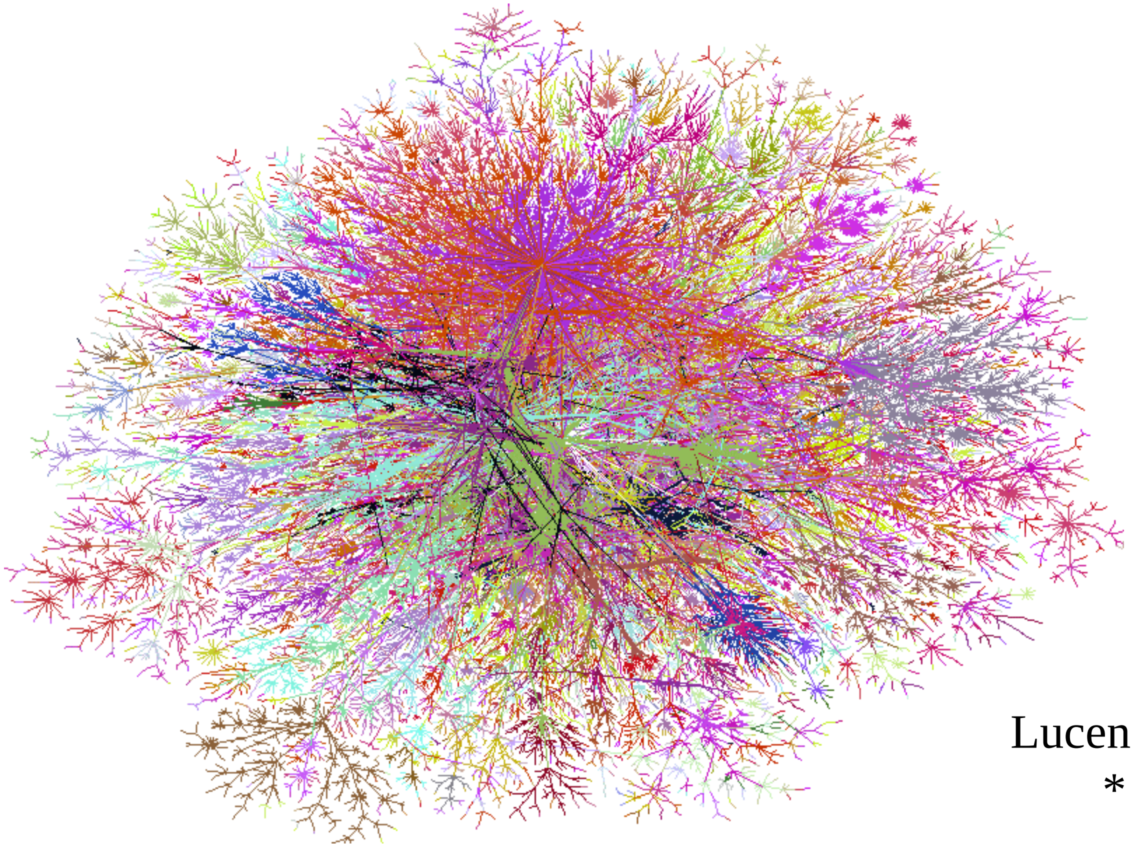
*Mr. George McMullin*
*USSTRATCOM/CL141*

# Silver Bullet ? ? ?

- Too early for Coors Light
- Not the Lone Ranger
- Certainly not killing werewolves
- Magic bullet – closer…but maybe not exactly

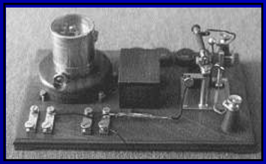
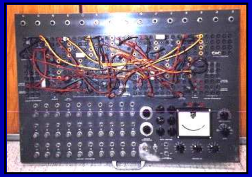
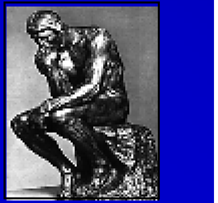
# The Challenge

- Growing dependence on information systems
- Rapid growth in computer networks
- Vulnerability to internal and external attack

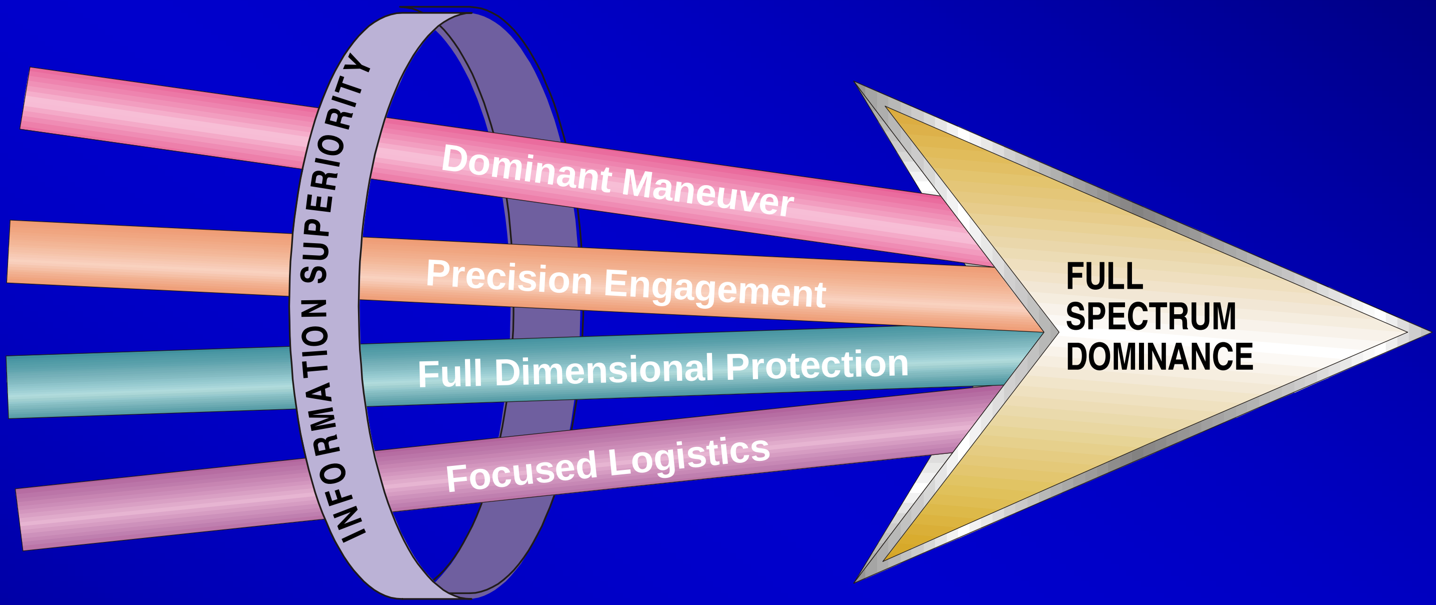


Lucent Technologies,
* 1996-2000

# Demand for Bandwidth

| | Civil War | WWI | WWII | Gulf War | Kosovo | AEF |
|---|---|---|---|---|---|---|
| | | | | | | |
| Data Transfer Rate | <32 BPS | 32 BPS | 71 BPS | 256 KBPS | 1.544 MBPS | ? Trillion BPS |
| Soldiers to Cover $10^2$ Km | 38,830 | 4,040 | 300 | 24 | 3 | ? |
| Time Line | 1865 | 1914 | 1945 | 1991 | 1999 | 2010 |
| Technology | |  |  | | |  |
| | Telegraph | Telephone | Computer | VTC | Web Tools | Cognitive Tools |

# Joint Vision 2020



**Dedicated individuals and innovative organizations transforming the joint force for the 21st Century to achieve *full spectrum dominance* :**

**- persuasive in peace**
**- decisive in war**
**- preeminent in any form of conflict**

# DoD IA Vision

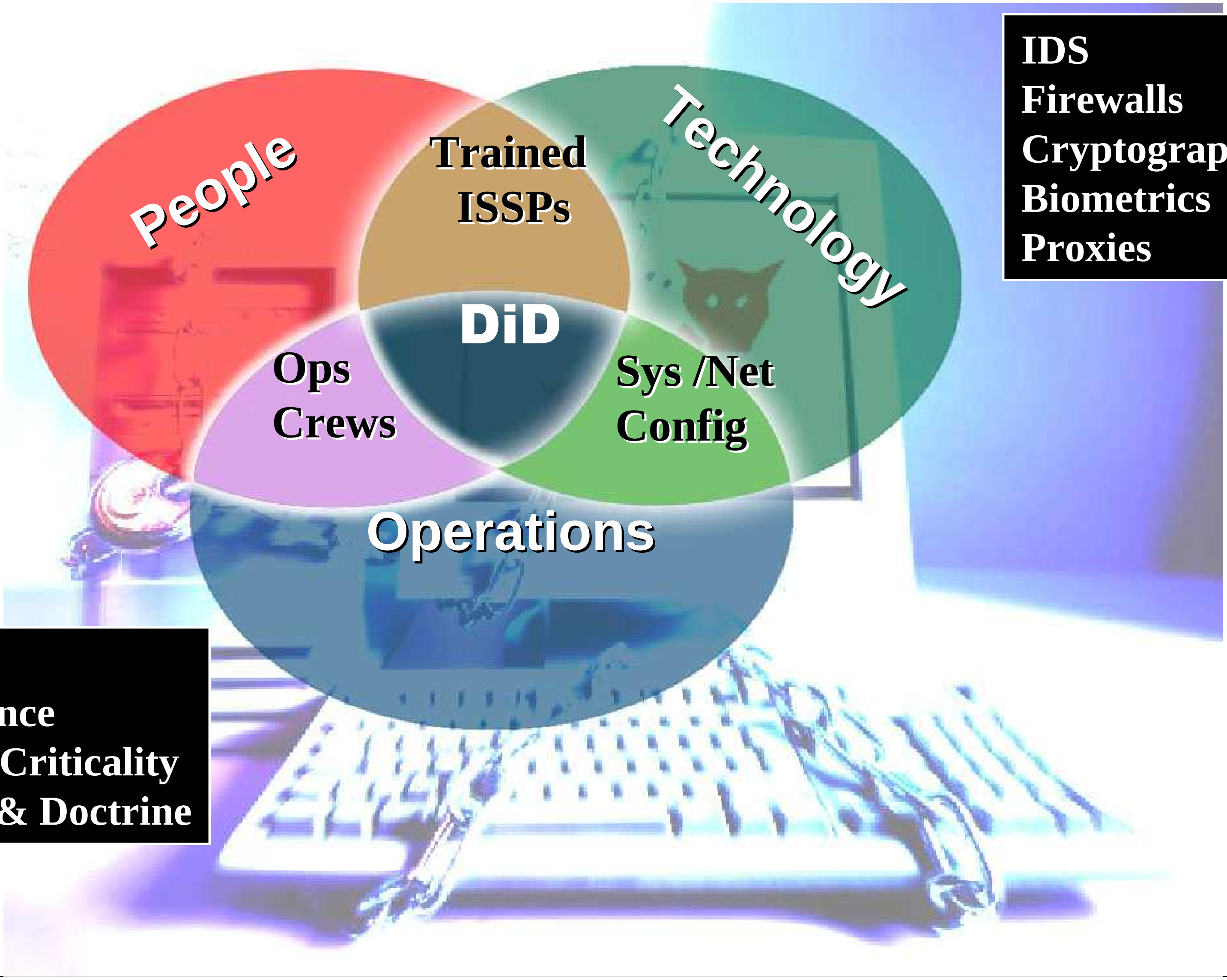
**Information Superiority for the DoD, achieved through a balanced integration of highly skilled personnel, operational policy and capability, and leading edge technology.**

***Information Assurance is essential to achieve and maintain Information Superiority.***

Ref: Defense Information Assurance Panel (DIAP), July 1998

# IA Model

Awareness
Training
Education
Experience
Certification



People

Technology

Operations

Trained
ISSPs

Ops
Crews

Sys /Net
Config

DiD

IDS
Firewalls
Cryptography
Biometrics
Proxies

I&W
Intelligence
Mission Criticality
Policies & Doctrine

# IA Goal

***Ensure critical DoD and command information resources are secure and protected***

Ref: DoD CIO October 1999, **DoD Information Management (IM) Strategic Plan** (ver 2.0)

# Information Assurance (IA)

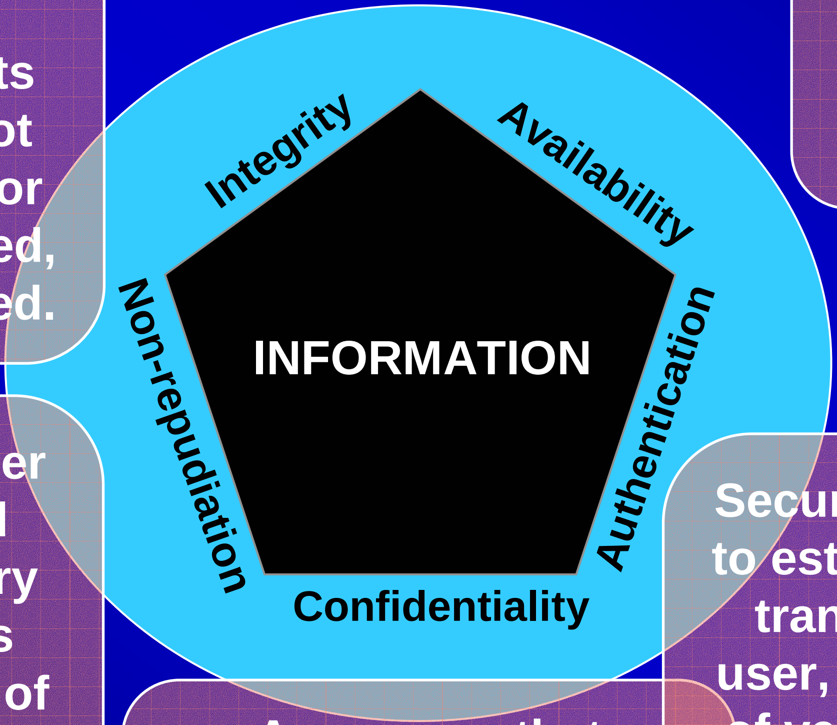
Information Assurance - “capabilities to maintain network availability, protect data integrity, and enforce authentication, confidentiality, and non-repudiation.”

Ref: CJCSI 6510.01

# Elements of Information Assurance

Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Timely, reliable access to data and information services for authorized users.



Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of origin, so neither can later deny having processed the data.

Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Security measure designed to establish the validity of a transmission, message, user, or system or a means of verifying an individual's authorization to receive specific categories of information.

# Information Assurance

## *Information Assurance* → *Mission Assurance*

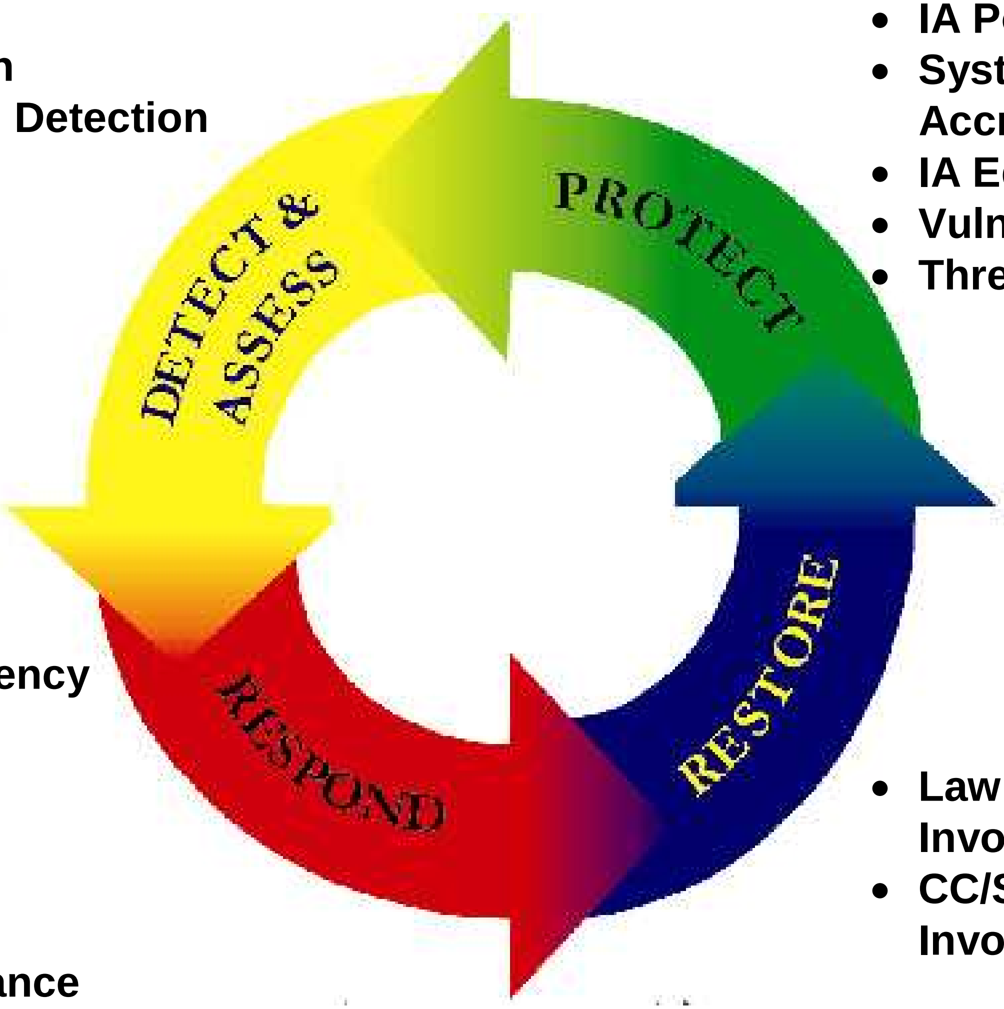
- **More than Information Protection**
- **Information Assurance ensures your network is available and operationally ready to provide:**
  - ***The right information***
  - ***At the right time***
  - ***In the right place***
  - ***In the right format***

***The Network is a Weapon System***

# CND Process

- Threat Identification
- Real Time Intrusion Detection
- Incident Reporting
- Intel/LE Integration

- IA Policies & Procedures
- System Certification & Accreditation
- IA Education & Training
- Vulnerability Assessment
- Threat Countermeasures



- Implement Contingency Plans
- Incident Response
- Exercise
- Plan & Policy Modification
- Restoration Assistance
- Post-attack analysis

- Law Enforcement Involvement
- CC/S/A CERT Involvement

# Information Assurance Challenges

- Interconnected, interdependent systems underscore need for broad understanding of threats and vulnerabilities
- Security-enabled commercial products - strong encryption with key recovery
- Global Security Management Infrastructure
- Cyber situation awareness - Cyber attack, sensing, warning and response capability
- Certify ALL users – from system administrators to common users

***Risk accepted by one may be imposed on all***

# Certification Mechanism

- Certification of Persons - ISO 17024, General Requirements for Bodies Operating Certification of Persons
  - Private organizations like the International Information Systems Security Certification Consortium
  - Government

# Partial Solution

- ‘No Silver Bullet’ – Will Poole, senior vice president of Microsoft’s Windows client division
- DoD Recognizes It
  - Vulnerability Management Process
  - Inspection Process
  - Service Provider Responsibility
- ‘Best Practice’ Standard

# Extreme Benefits

- Minimizes ‘stupid user tricks’
- Reduces potential business cost
- Raises overall awareness
- Increases your network police force
- Improves security of entire internet
- Reduces potential business cost

# NSA Centers of Excellence for Information Assurance Education

## *3 DoD Institutions*

Naval Postgraduate School

United States Military Academy, West Point

Information Resources Mgmt College (IRMC) / National Defense University (NDU)

## *21 Public / Private Non-DoD Institutions*

Carnegie Mellon

Florida State

George Mason University

Idaho State

Iowa State <<<

James Madison University

Drexel University

University of Maryland (Baltimore County)

University of North Carolina, Charlotte

West Virginia University

Georgia Institute of Technology

Syracuse University

Purdue University

Stanford

UC Davis

University of Illinois

University of Idaho

University of Nebraska <<<

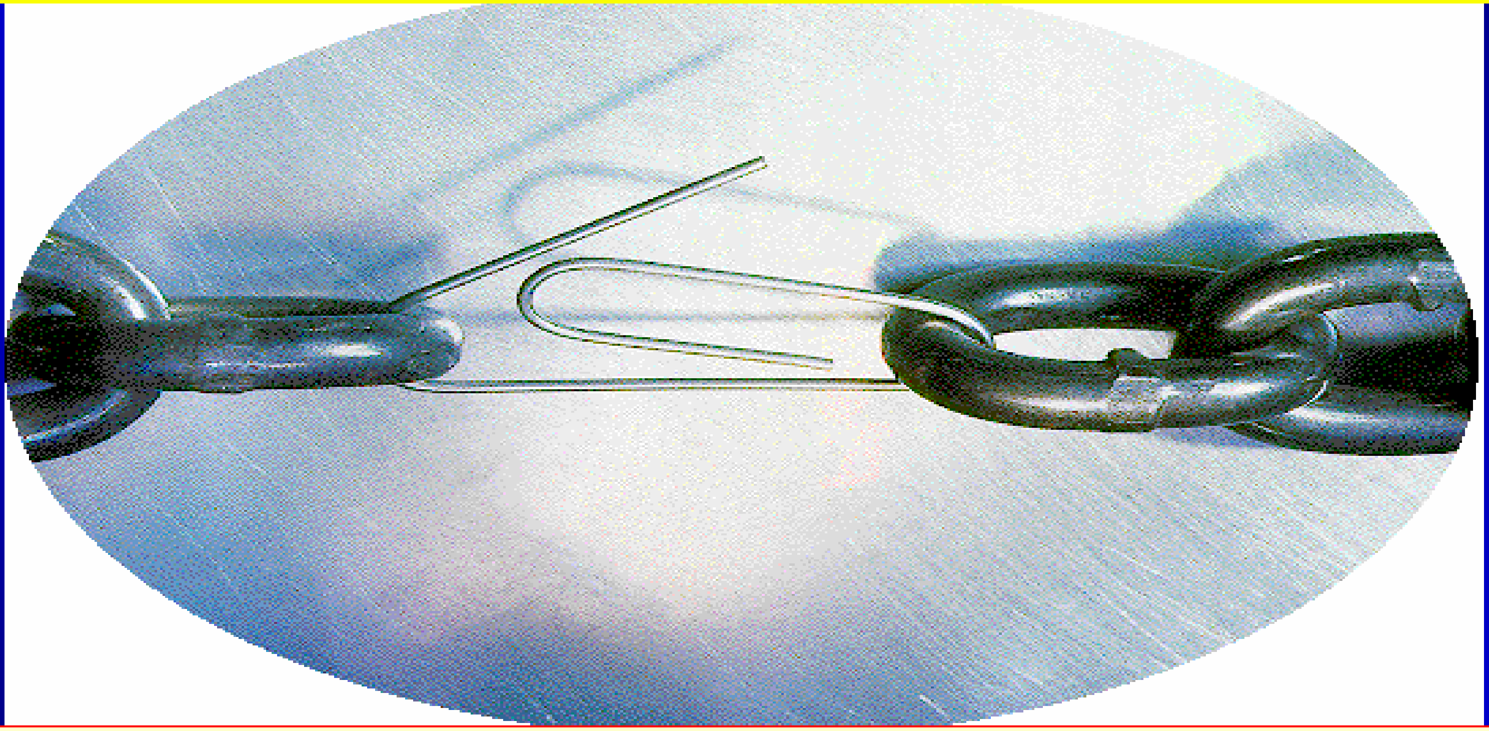
University of Tulsa

Mississippi State University

Norwich University

# The Weak Link

***A Risk Accepted By One May Be Imposed On All***



***In IA we’re only as strong as our weakest link!***

# United States Strategic Command