Security on the Desktop

Fighting the Enemy Within

GovTechNet 99-15 June 99

Army Research Laboratory

Adelphi Lab Center (ARL-ALC)

LTC Paul Walczak
(301) 394-3862 DSN 290
pwalczak@arl.mil

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 15061999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Security on the Desktop Fighting the Enemy Within	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Army Research Laboratory Adelphi Lab Center (ARL-ALC)	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 10	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	6/15/99	Briefing

4. TITLE AND SUBTITLE
Security on the Desktop, Fighting the Enemy Within

5. FUNDING NUMBERS

6. AUTHOR(S)
LtCol Paul Walczak

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This briefing entitled “Security on the Desktop: Fighting the Enemy Within” was presented by LTC Paul Walczak, of the Army Research Laboratory to GovTechNet 99 in June 1999. It examines the scope of the challenges of securing Army information and information networks and provides some examination of some of the INFOSEC research areas that will tackle this problem.

14. SUBJECT TERMS
INFOSEC

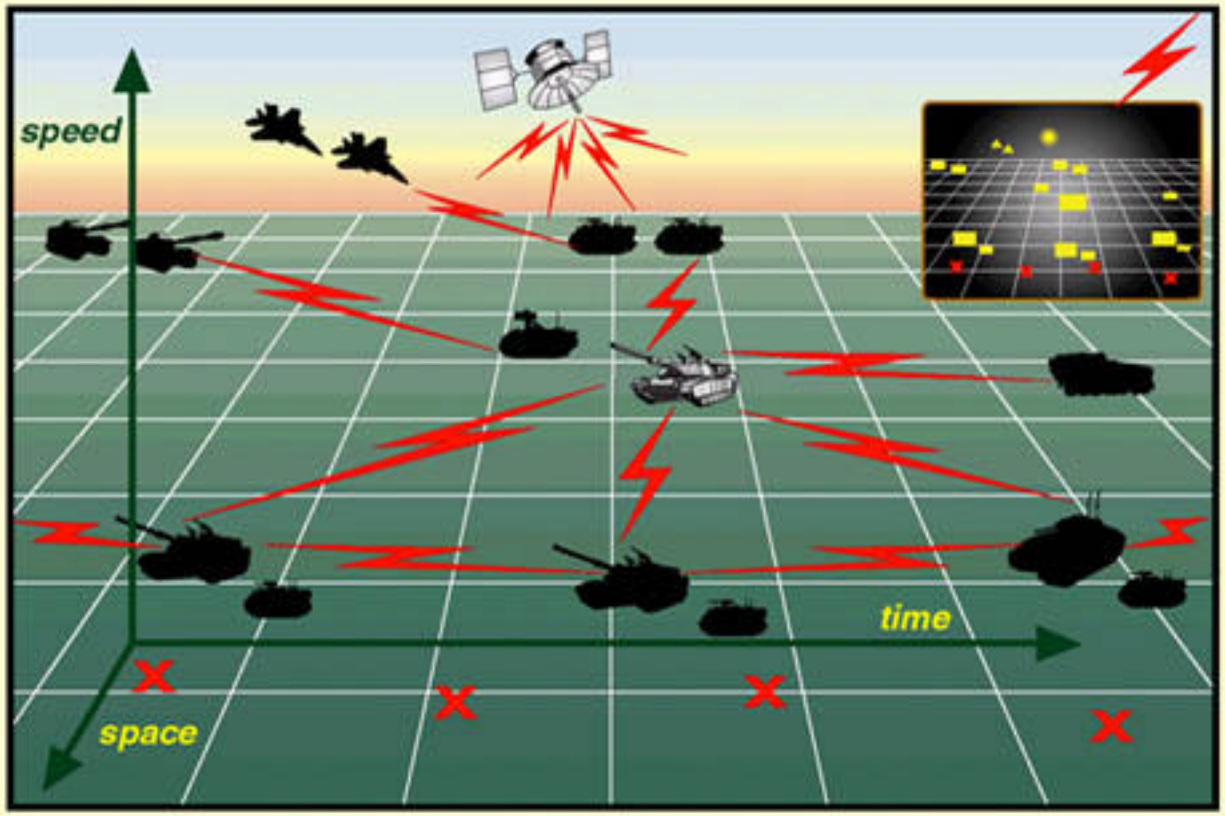
15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Army XXI - *Into the Future*

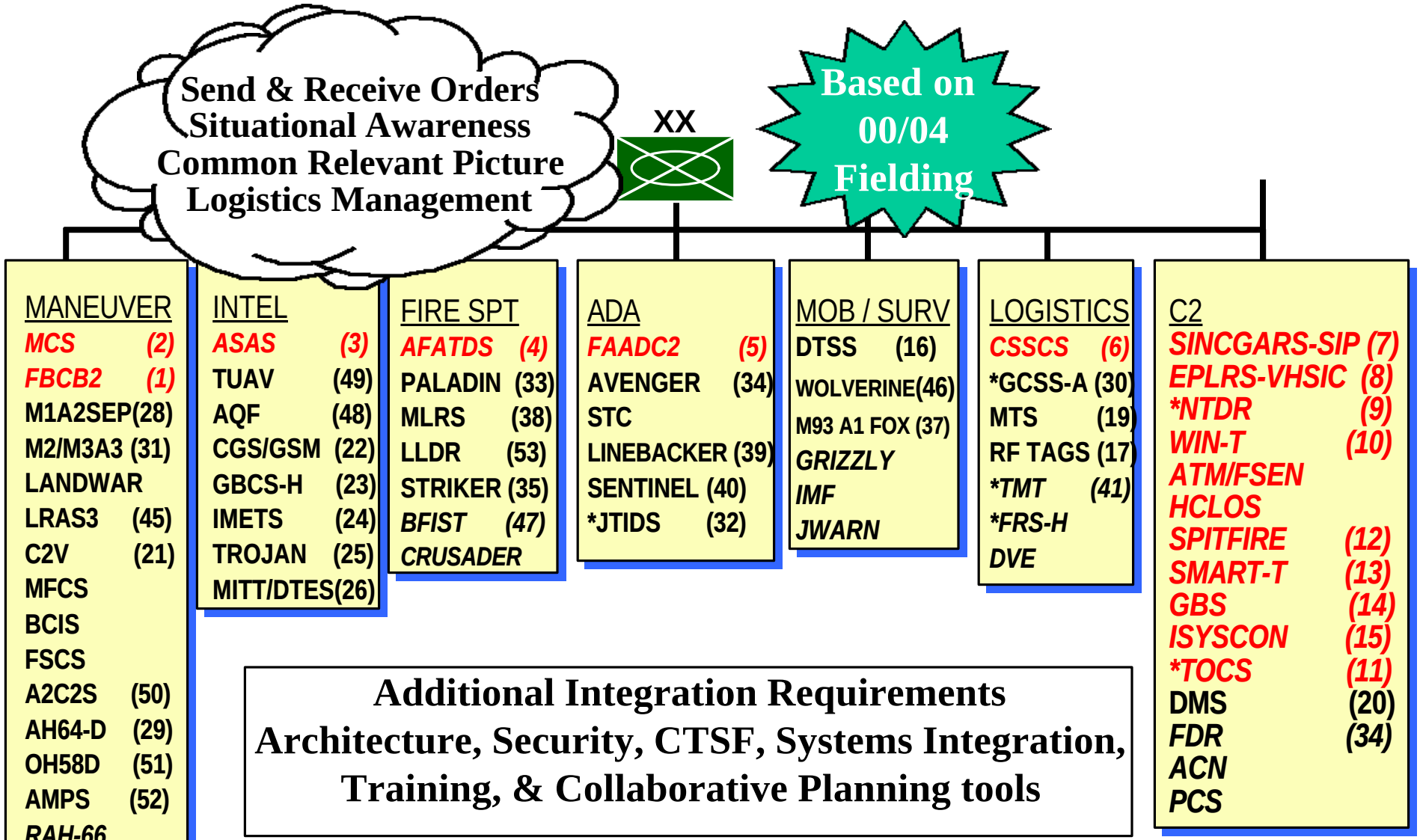
The Incorporation of Digital Technology Across All Of Our Battlefield Systems Will Give Commanders And Soldiers Unprecedented Capability to Gather And Share Tactical Information



PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, AND COMMUNICATIONS SYSTEMS 8/28/97 0005

Slide Courtesy of US Army PEOC3S

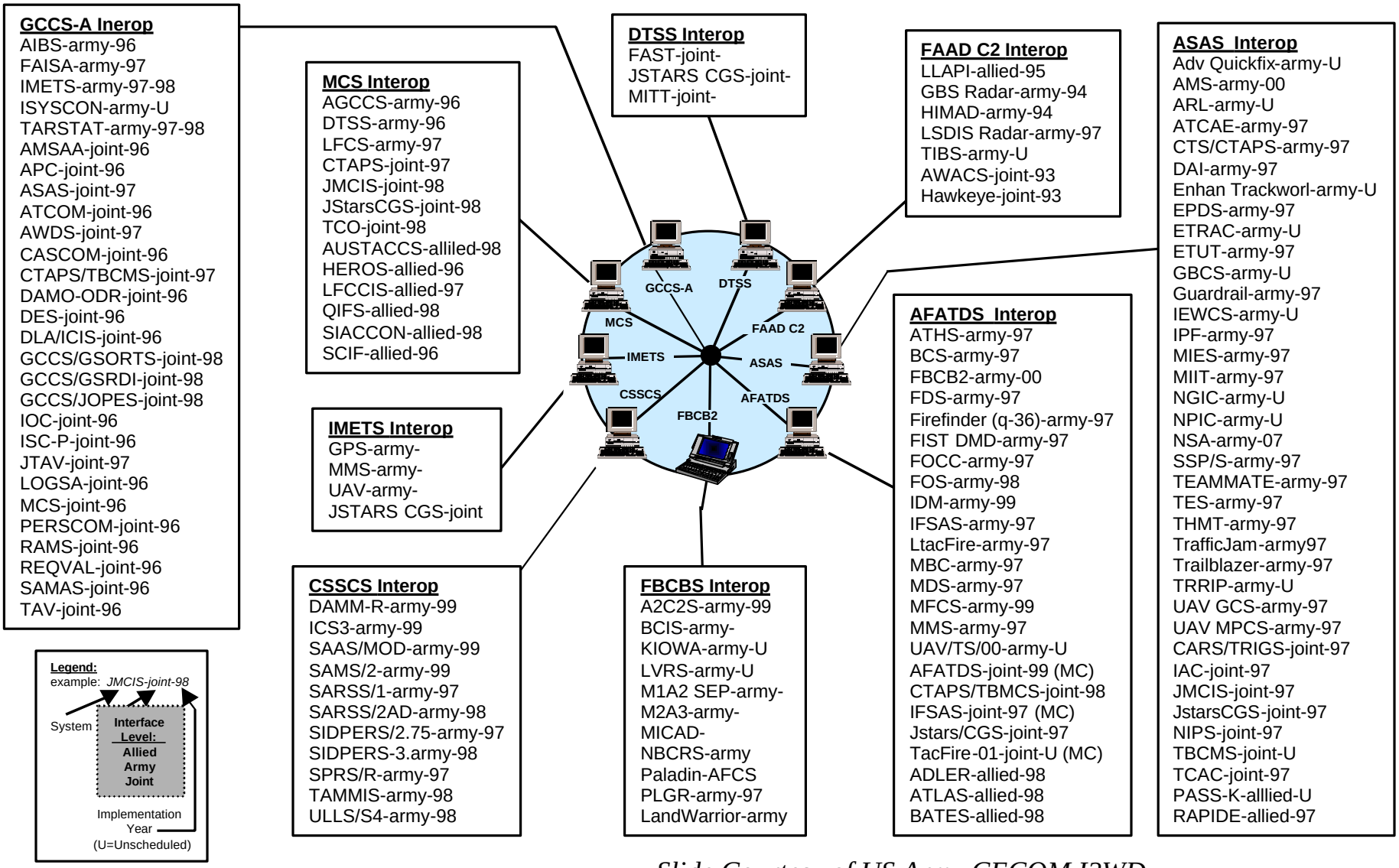
U.S. Army Near Term Requirements
FDD Division Chart



Additional Integration Requirements
Architecture, Security, CTSF, Systems Integration, Training, & Collaborative Planning tools

Slide Courtesy of US Army CECOM I2WD

U.S. Army Objective Requirements
ABCS Systems/Networks Chart



Slide Courtesy of US Army CECOM I2WD

Partial View to Problem's Scale

Army Information Systems 14,544

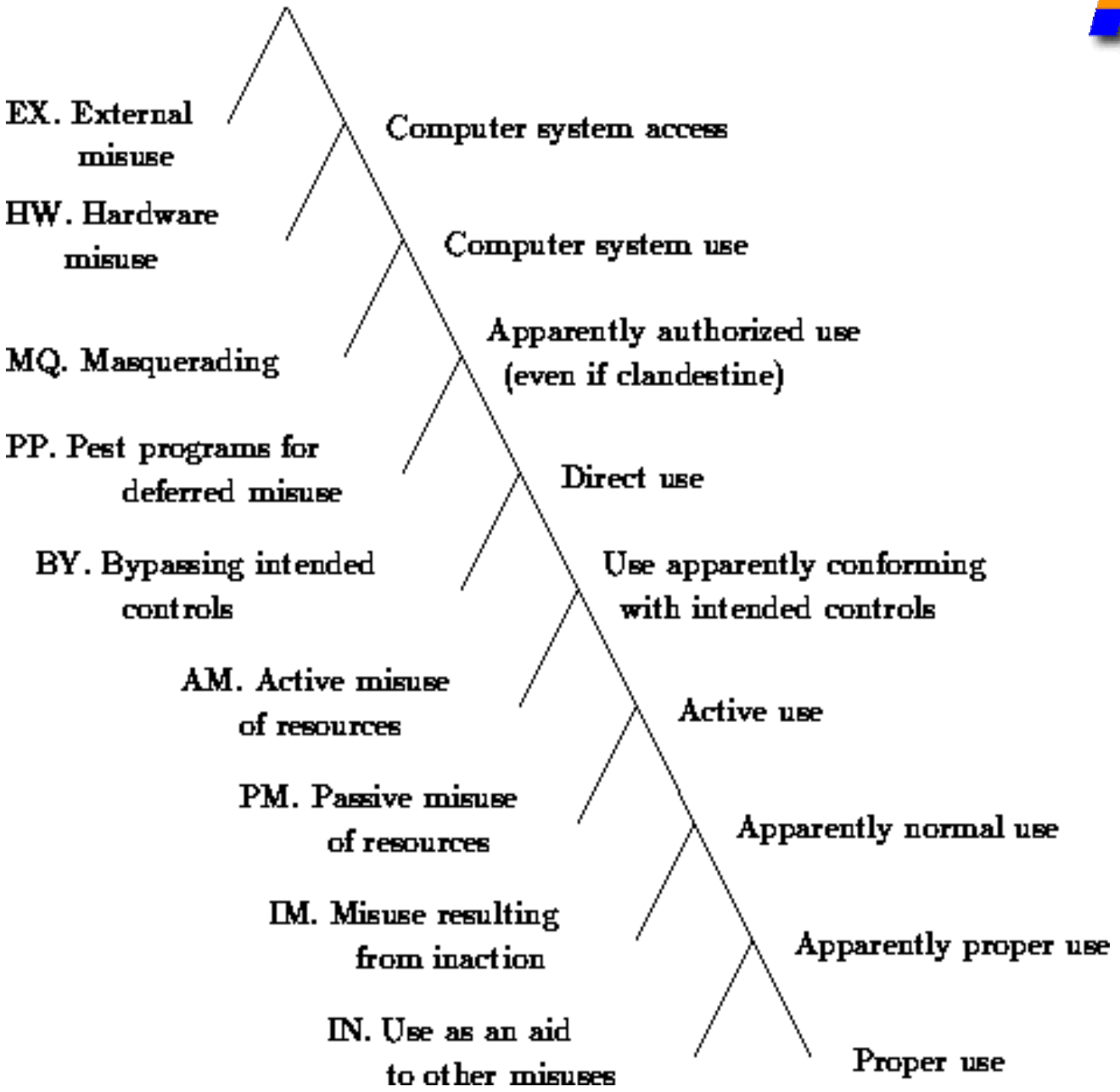
- Major Systems 1,219
  - Mission Critical 638
  - Other Major 581
- Other Systems (996 Web sites) 13,325

Information Technology Controlled Devices 444,196

- PCs/Servers 365,077
- Facilities & Other 42,048
- Communications Hardware/Software 7,071

Army IS Security Program (total funding) $ 87 million

Classes of Computer Misuse Techniques



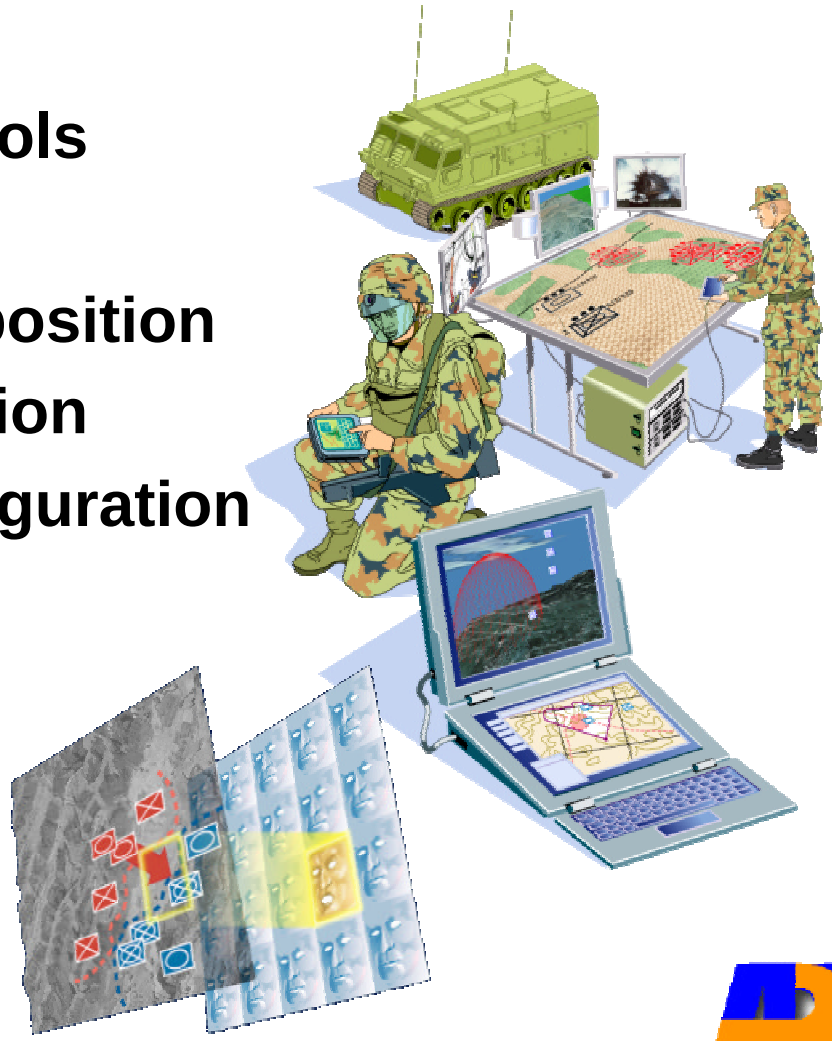
Securing Systems at the Desktop

- ✦ Insider Misuse
- ✦ Development Practice
- ✦ Threat is Learning
- ✦ Warrior's "desktop"
- ✦ Assurance >> Securing Systems
- ✦ Process and Culture

- ❑ Holistic interpretation
- ❑ Acquisition Strategy
- ❑ Education, Training
- ❑ Spectrum of Information
- ❑ Overarching concept for INFOSURV
- ❑ No silver bullets

Directions for INFOSURV R&D

1. Robust networking protocols
2. Requirements metrics
3. Predictable systems composition
4. Data analysis and correlation
5. Dynamic system (re) configuration
6. Dynamic adaptability
7. Architectures
8. Mobile code
9. Components



INFOSEC Research Areas

1 -Security Engineering Methodologies

2 -Detecting Intrusion and Misuse

3 -Mobile, Foreign Code

4 -Controlled Sharing

5 -Denial of Service

6 -Application Security

7 -Communications Security

8 -Security in Mobile Environments

9 -Security Management Infrastructure