GENERAL DYNAMICS
Advanced Information Systems

Rethinking Defensive Information Warfare

Geoffrey S. French

Overview

- **Current state of DIW**
  - Doctrine
  - Theory
  - Practice
- **Fundamental Flaws in Information Assurance (IA)**
  - Technical and logical shortcomings
  - Limits of cyber risk management
- **New Basis for DIW**

DIW Defined

Joint Pub 3-13

The integration and coordination of policy, personnel, and technology to protect information and information systems.

IA, physical security, OPSEC, counter-deception, counter-psyops, CI, EW, and special information operations.

Ensure access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes

DIW Explained

- OPSEC and risk management
- Protection, detection, restoration, and response

DIW Expanded

- Defensive counterinformation
- Counter propaganda and public affairs
- Protection of any information-based process in military activity

DIW Doctrine

- **Emphasis is on passive monitoring and basic OPSEC procedures**
- **Generic risk management methodology**
- **No guidance for**
  - preparations for improving defense prior to an attack
  - response to a cyber attack in wartime conditions

DIW Theory: NCI Focus

- **1996 NDU Study**
  - Addressed defense of national critical infrastructure (NCI) as well as military
  - Acknowledges that poor ability to identify which assets are critical
  - Recommends raising level of defense to meet the sophistication of the attack

DIW Theory: DII-Focus

- **1999 RAND study**
  - Addressed Defense Information Infrastructure
  - Called for definition of “minimum essential”
  - Acknowledged that “just about everything must be included”
  - Set up six-step risk management process

Defense Science Board Studies

- **1996 Report**
  - Looked at both DII and NCI
  - Called for improvements in basic functions (warning, damage assessment)
- **2001 Report**
  - Looked at DII
  - Called for stronger architecture in the Global Information Grid, better intrusion detection, and increased R&D

DoD cannot today defend itself from an Information Operations attack

Defense Science Board, 2001

Current State of Practice

- **Expansion of term, focus on day-to-day operations and computer network defense (CND)**
  - Monitoring for intrusions
  - Identifying malware
  - Installing patches
  - Incident response
- **Emphasis on IA**

Is IA a Solid Foundation?

- **Based on ideals**
  - Flawless software
  - Flawless implementation and configuration
  - Up-to-date patches and signatures
  - Access limited to authorized users
  - Users have appropriate privileges
  - No one undermining security

Hardware and Software

- **In reality**
  - Operating Systems (e.g., Windows)
  - Fundamental Services (e.g., BIND)
  - Applications (e.g., IIS)
- **Flaws exist**
  - Not just announced and patched vulnerabilities
  - Undiscovered flaws

The patch model for Internet security has failed spectacularly.

Caida, 2004

Signature-Based Defense

- **Anti virus, intrusion detection, firewalls**
  - Rules are set up to identify known characteristics of existing exploits or malware
- **By definition, reactive**
- **Cannot stop the zero-day exploit or the latest worm**

Authentication

- **Most networks require simple authentication**
  - Username
  - Password
- **Passwords are notoriously insecure**
- **Moving toward “single sign-on”**
- **Poor verification of authorized use of network**

The Reality of Complexity

- **In theory, network security should be straightforward**
- **In practice, it is complex**
  - Interactions of hardware, software
  - Mobile users
  - Personal equipment
- **There are individual solutions to each problem, but each solution has its own vulnerabilities and problems**

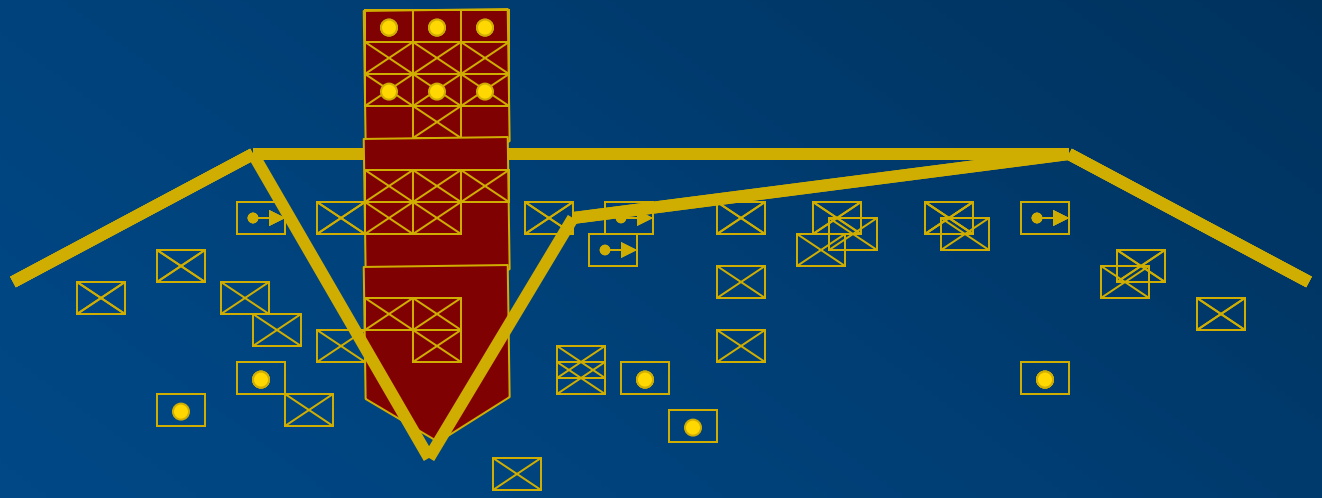
Implications for Risk Management

- **Poor definition of "critical" assets**
  - May be no differentiation
- **In peacetime, risk may be acceptable**
  - Time to investigate intrusions
  - Personnel to respond to incidents
- **In wartime, the risk is unacceptable**
  - Against a sophisticated adversary, IA certain to fail
  - A small amount of wrong of unavailable data can have a large impact on military decisions

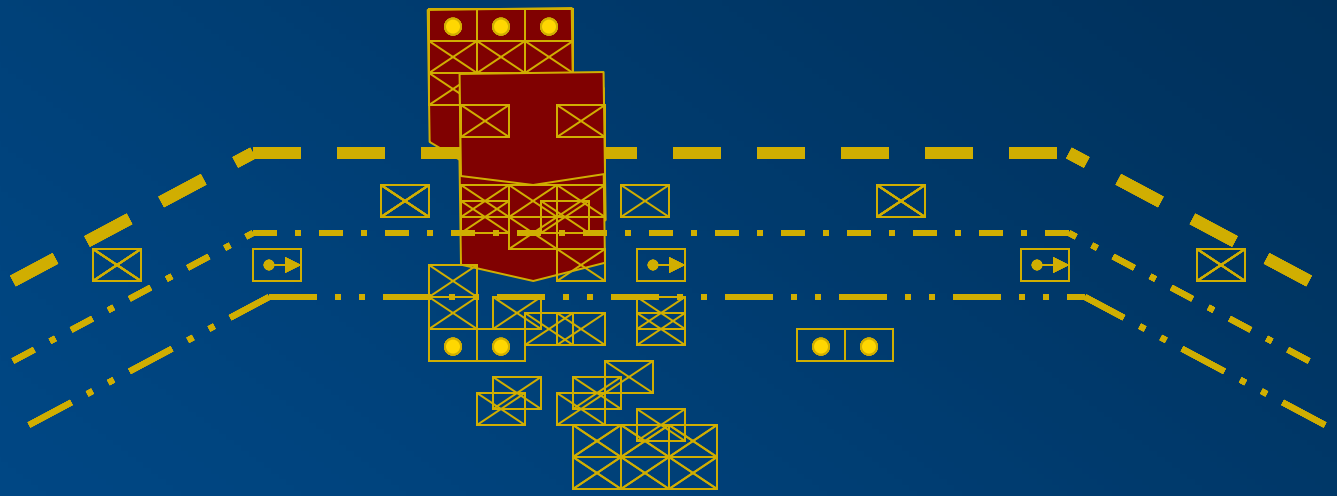
New Basis for DIW

- **Examine military history**
- **Draw analogies**
  - Perimeter defense unlikely to succeed
  - Limited ability to counterattack
- **Historical examples**
  - German defense in depth from WWI
  - American active defense from Cold War
  - Serbian defense of NATO Kosovo air campaign

WWI Perimeter Defense



WWI Defense in Depth

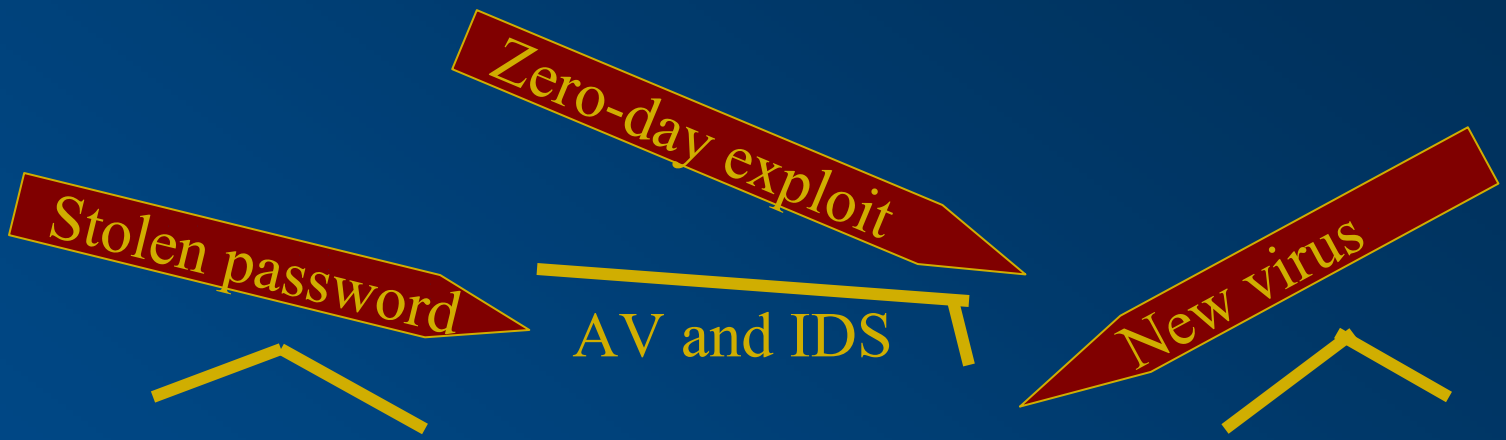


Lessons Drawn

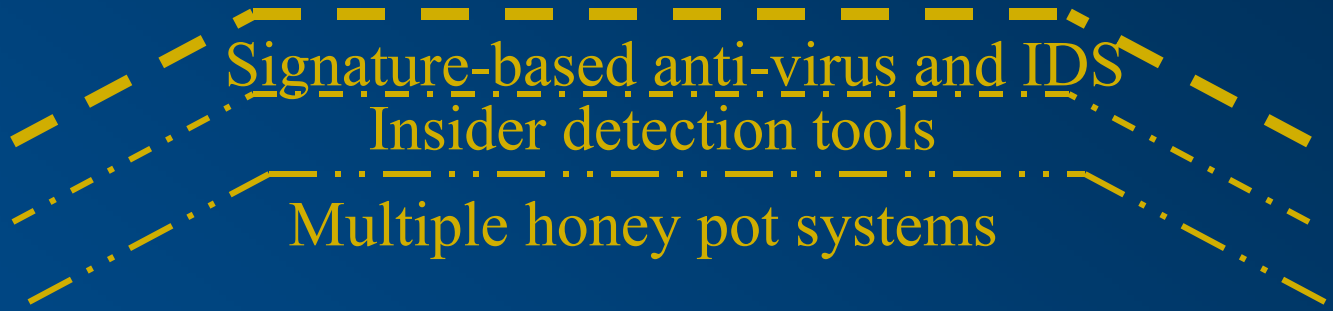
- Even with forward-deployed forces, perimeter will be penetrated
- Detection and reaction are part of defense

Network Perimeter Defense

Network Perimeter Defense



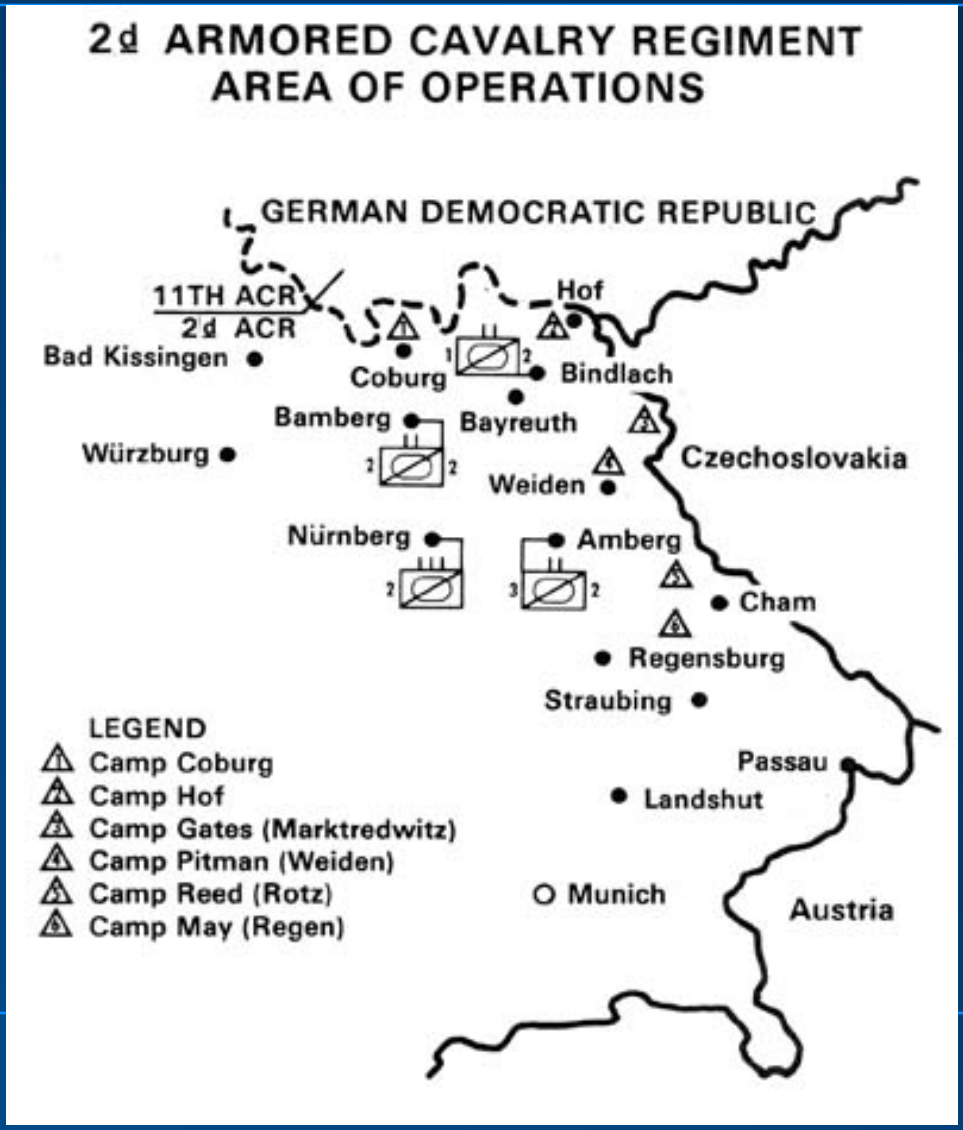
Network Defense in Depth



From Forward Defense to Active Defense

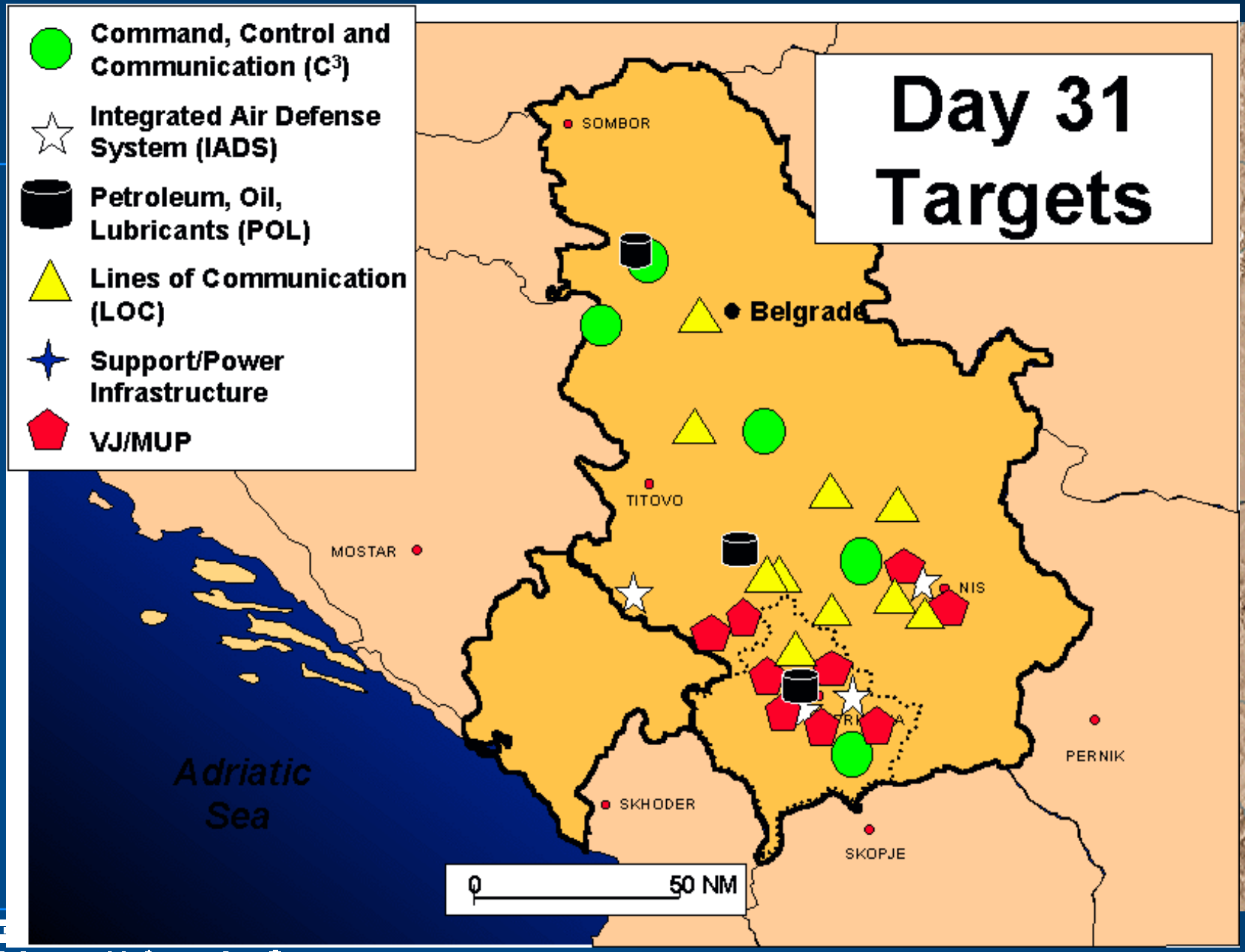
- **US faced numerically superior foe**
- **Active Defense**
  - Firepower disadvantage
  - Knew forward positions would be overrun
  - Response: hardening combined with mobility

Cold War: European Defense



Active Network Defense

- **Hardening**
  - Locked down operating system
    - Rigid execution control
- **Mobility**
  - Countering adversary reconnaissance
  - Changes in
    - IP addresses
    - Configuration (including DNS and BGP)
    - Equipment



Advanced Information Systems

Source: Global Security

Lessons drawn

- **Deception and denial**
  - Neutralize enemy firepower advantage by countering intelligence, surveillance, and reconnaissance

Network-based Deception

- **Not necessarily honeypots**
- **Targeted at adversary reconnaissance**
  - Simulated responses
  - Diverted traffic to real networks
- **Should be tailored**
  - Could draw in adversary
  - Could discourage adversary
- **Should be centrally controlled**

Integration

- **If combined**
  - Counter pre-crisis adversary reconnaissance with mobility
  - Counter reconnaissance during crisis or war with deception
  - Detect insider threat and network penetration
  - Harden certain systems to better protect critical systems
- **Prepare DoD systems for war**

Summary

- IW has lost emphasis on war
- DIW has lost any concept of escalation for crisis or conflict
- Military history can illustrate adaptations in the face of adversity
- DIW needs to look to military history to reinvigorate review of strategic needs