



Cyber Threat to Critical Infrastructure

*Special Agent Jim Christy (AFOSI)
Law Enforcement & Counterintelligence Coordinator*

*Defense-Wide Information Assurance Program
Assistant Secretary of Defense
Command, Control, Communications, and Intelligence (ASDC3I)*

Defense-Wide Information Assurance Program



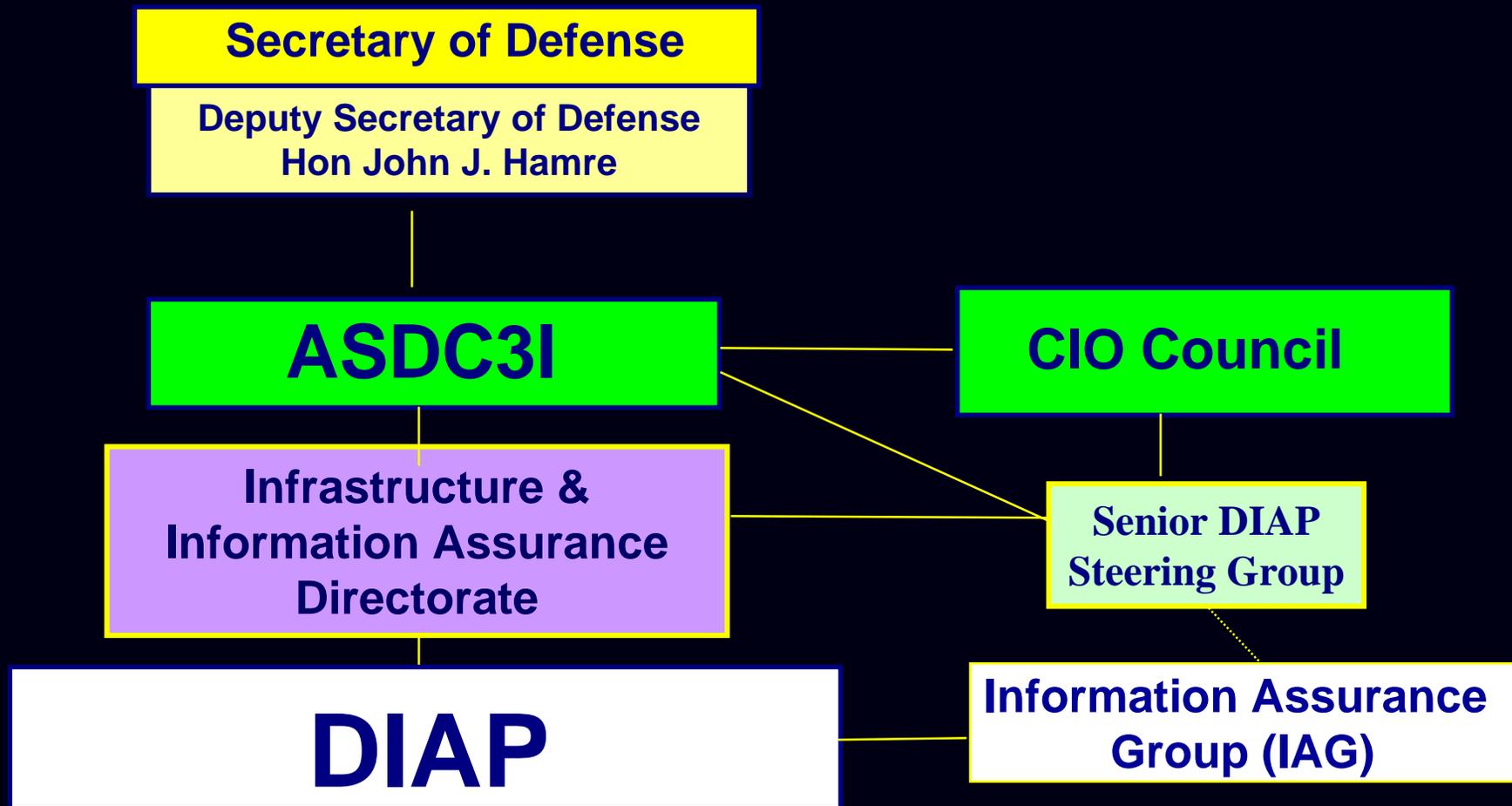
Overview

- *DIAP*
- *Crime Vs Info War*
- *Legal Issues*
- *Senate Hearings*
- *CND*
- *Law Enforcement Recommendations*

Defense-Wide Information Assurance Program



ASDC3I/DIAP



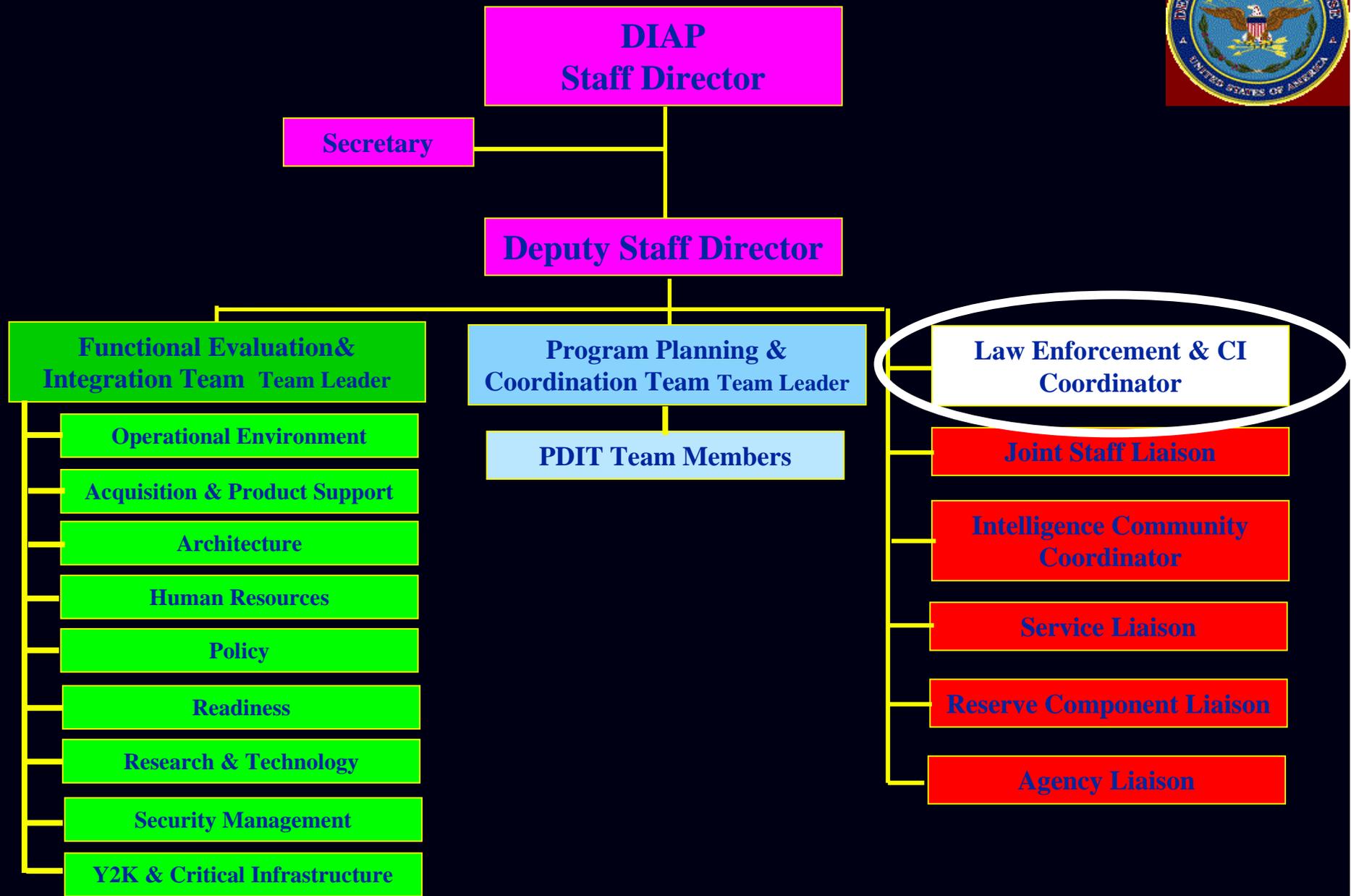
Defense-Wide Information Assurance Program



DIAP Mission

The Defense-wide Information Assurance Program (DIAP) provides for the planning, coordination, integration, and oversight of the Department's Information Assurance resources to assure the availability, integrity, authentication, confidentiality, and non-repudiation of the Department's mission essential and mission support information.

Defense-Wide Information Assurance Program



Defense-Wide Information Assurance Program



**DIAP
Staff Director**

Secretary

Deputy Staff Director

**Functional Evaluation &
Integration Team Team Leader**

**Program Planning &
Coordination Team Team Leader**

**Law Enforcement & CI
Coordinator**

Operational Environment

PDIT Team Members

Joint Staff Liaison

Acquisition & Product Support

Architecture

Human Resources

Policy

Readiness

Research & Technology

Security Management

Y2K & Critical Infrastructure

**Intelligence Community
Coordinator**

Service Liaison

Reserve Component Liaison

Agency Liaison

Manpower Total = 11

All Positions 1 Deep

 Vacant

 Part-Time

Defense-Wide Information Assurance Program

Crime vs. InfoWar - The Legal Issues

- *Who is Perpetrator?*

- *Criminal? Terrorist? State-Sponsored Terrorist? State?*

- *Where is the Perpetrator?*

- *US? International Waters/Airspace? Third Country? State of Perpetrator?*

- *What is the Impact on the U.S.?*

Minor Disruption

Damage to National Security



- *Who Should Respond (Stop the Attack)?*

- *LE? Host Country? U.S. Military?*

Perpetrator

*Criminal *Terrorist * State Sponsored Terrorist *State

Location

U.S

International
Water/Air

3rd Party
Country

State

U.S. Impact

Minor Economic
comms disruption

Minor Economic
comms disruption
with loss of life

Major Economic
comms disruption

Major Economic
comms disruption
with loss of life

Damage to
National
Security

Right to Respond

U.S. Law
Enforcement

Host Country
or Flag State
Law Enforcement

U.S. Military

Perpetrator

*Criminal *Terrorist * State Sponsored Terrorist *State

Location

U.S

International
Water/Air

3rd Party
Country

State

U.S. Impact

Minor Economic
comms disruption

Minor Economic
comms disruption
with loss of life

Major Economic
comms disruption

Major Economic
comms disruption
with loss of life

Damage to
National
Security

Right to Respond

U.S. Law
Enforcement

Host Country
or Flag State
Law Enforcement

U.S. Military
if DOJ/FBI Cert
& Pres Exec Order

Perpetrator *Criminal *Terrorist * State Sponsored Terrorist *State

Location

U.S

International
Water/Air

3rd Party
Country

State

U.S. Impact

Minor Economic
comms disruption

Minor Economic
comms disruption
with loss of life

Major Economic
comms disruption

Major Economic
comms disruption
with loss of life

Damage to
National
Security

Right to Respond

U.S. Law
Enforcement

Host Country
or Flag State
Law Enforcement

U.S. Military
if DOJ/FBI Cert
& Pres Exec Order

Perpetrator *Criminal *Terrorist * State Sponsored Terrorist *State

Location

U.S

International
Water/Air

3rd Party
Country

State

U.S. Impact

Minor Economic
comms disruption

Minor Economic
comms disruption
with loss of life

Major Economic
comms disruption

Major Economic
comms disruption
with loss of life

Damage to
National
Security

Right to Respond

U.S. Law
Enforcement

Host Country
or Flag State
Law Enforcement

U.S. Military
W/NCA
Permission

Perpetrator *Criminal *Terrorist * State Sponsored Terrorist *State

Location

U.S

International
Water/Air

3rd Party
Country

State

U.S. Impact

Minor Economic
comms disruption

Minor Economic
comms disruption
with loss of life

Major Economic
comms disruption

Major Economic
comms disruption
with loss of life

Damage to
National
Security

Right to Respond

U.S. Law
Enforcement

Host Country
or Flag State
Law Enforcement

U.S. Military
W/NCA
Permission



Facts

- *We Will Face Competent Adversary*
 - *We Won't Know the Perpetrator*
 - *We Won't Know the Location of the Perpetrator*
- *Law Enforcement Will Always Have Primary Jurisdiction Until Perpetrator & Location are Determined*

Defense-Wide Information Assurance Program



Need to Prepare

- *New Adversaries*
 - *Virtual Organizations*
 - *Non-Traditional Threats*

Defense-Wide Information Assurance Program



InfoWar Attacks



**Cyber Terrorism
Attacks**



Criminal Incidents

Number of Actual Incidents

Defense-Wide Information Assurance Program



Resources & Expertise

**DoD CERTS, CIA, DIA, J2, NSA
InfoWar Centers**

Law Enforcement →
& Counterintelligence

Defense-Wide Information Assurance Program



Resources & Expertise

**DoD CERTS, CIA, DIA, J2, NSA
InfoWar Centers**

Law Enforcement →
& Counterintelligence

Defense-Wide Information Assurance Program



Assumptions

- Intelligence Community Restricted in U.S.*
- The Vast Majority of Attacks Will Involve U.S. Systems (Civilian/Non-Gov)*
- Every Intrusion is a Crime*
- Over 95% DOD Information over PSN*
- Imperative to Trace Attacks Back to Source*

Defense-Wide Information Assurance Program



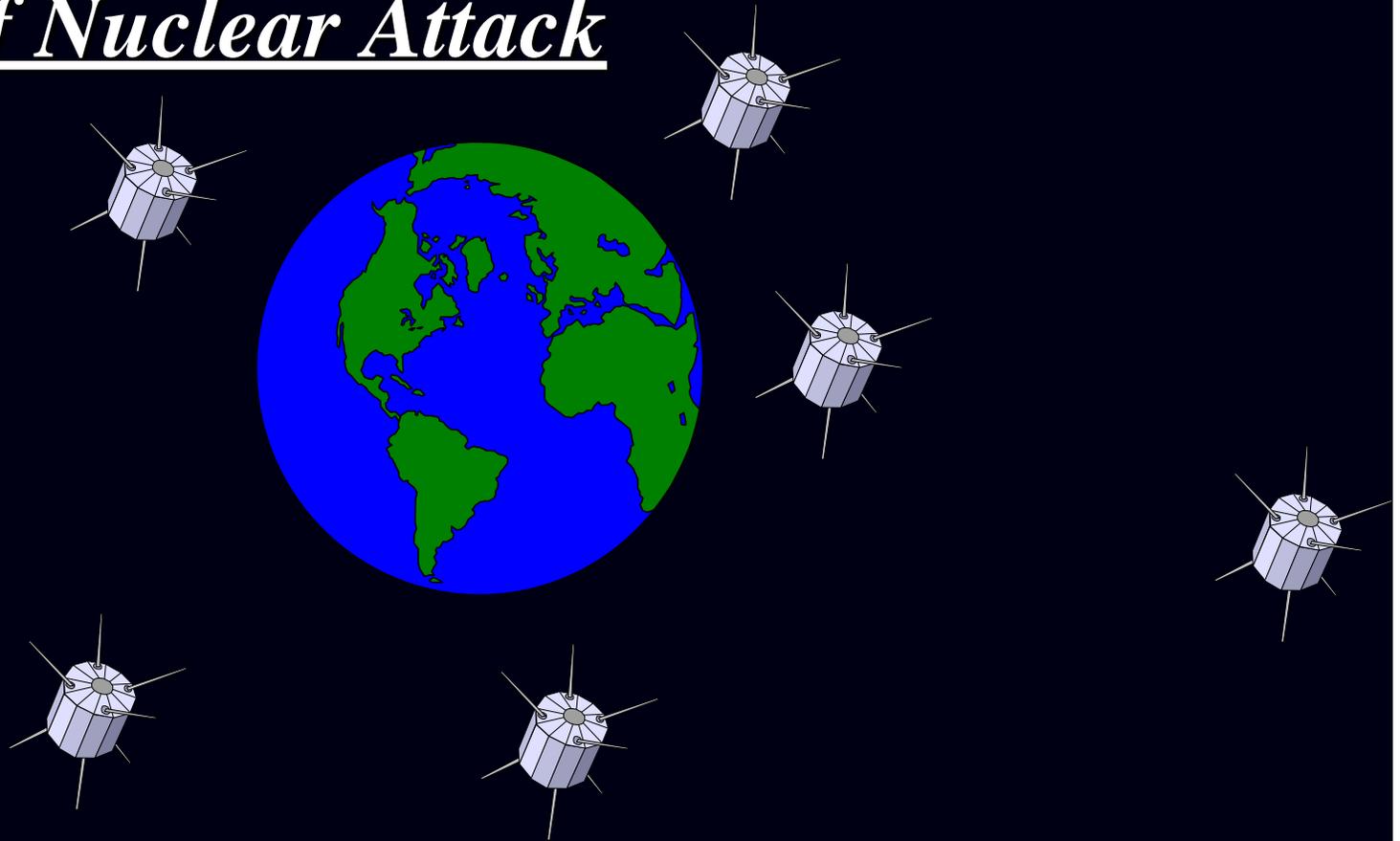
Attack Profile

- *Will Probably Look Like Multiple Unrelated Incidents (All Criminal Incidents) Initially*
- *Will Probably Attack Civilian Infrastructure, Not DOD - 20th Century Fox Project - "WorldWar3.com"*
- *Launched from US or Allied Country*

Defense-Wide Information Assurance Program



Opposite of Nuclear Attack



Defense-Wide Information Assurance Program



Opposite of Nuclear Attack



Defense-Wide Information Assurance Program



Criminal Violations:

- 18 USC 1029, Access Device Fraud*
- 18 USC 1030, Computer Fraud Act*
- 18 USC 2511, Interception & Disclosure of Wire,
Oral or Electronic Communication*
- 18 USC 2701, Stored Wire & Communication
Access*

Defense-Wide Information Assurance Program



Criminal Violations (cont'd):

- 18 USC 785 - Threats*
- 18 USC 1343 - Wire Fraud*
- 18 USC 1363 - Malicious Mischief*
- 18 USC 1462 - Import of Obscene Matter*
- 18 USC 1465 - Transport of Obscene Matter*
- 18 USC 2252 - Sexual Exploitation of Minors*
- 18 USC 2314 - Transport of Stolen Property*



Criminal Violations (cont'd):

- 18 USC 2319 - Copyright Infringement*
- 18 USC 2320 - Trademark Goods*
- 18 USC 2510 thru 2521 - Wiretaps*
- 18 USC 2701 thru 2711 - Stored Electronic Comm*
- 18 USC 3121 - Pen Registers*
- 17 USC 506 - Copyright Infringement*
- 42 USC 2000aa - Privacy Protection*

Defense-Wide Information Assurance Program



The Problem

“18th Century Law & 20th Century Technology”

*Col. Bob Giovagnoni
AFOSI, JA
1996*



Defense-Wide Information Assurance Program



The First Problem

Speed Counts!



Defense-Wide Information Assurance Program



The Second Problem

The Legal Environment is

Geo-Centric



Defense-Wide Information Assurance Program



The Law

- *Criminal Law - Law Dealing with Crime & Punishment*
- *Procedural Law - Legal Procedures Required of a Law Enforcement Official for the Commencement of Legal Proceedings*





Criminal Law

- What is a Crime

- What is Against the Law

*i.e. Rape, Murder, Fraud, Computer Intrusions,
Narcotics Trafficking, etc..*



Defense-Wide Information Assurance Program



Procedural Law

- How to Collect Evidence

- Wire Tap Court Orders

- Search Warrants

- Rights Advisements



Defense-Wide Information Assurance Program



Procedural Law

Balance Between

- Individual Rights of Privacy

- Public Safety



Defense-Wide Information Assurance Program

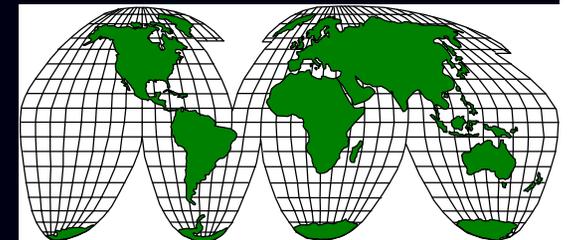


International Cooperation

- Each Country's Legal Infrastructure

- Sovereignty

- Mutual Assistance Agreements



Defense-Wide Information Assurance Program

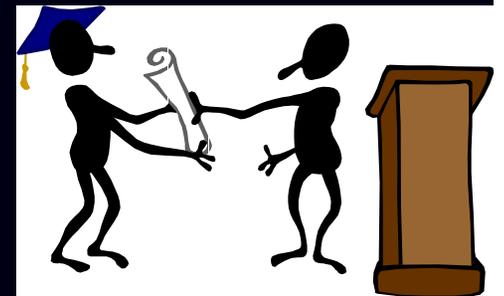


Your 3rd Grade Teacher was Right

*There's a **BIG** Difference Between*

What You CAN DO &

What You MAY DO



Defense-Wide Information Assurance Program



Your 3rd Grade Teacher was Right

CAN - *To Be Able to*

- *To Have the Knowledge or Skill to*

- *To Know How to*

- *To Be Mentally Able to*

MAY - *Have Permission to*

- *Be Free to*

- *Be Achieved Within a Democratic Framework*

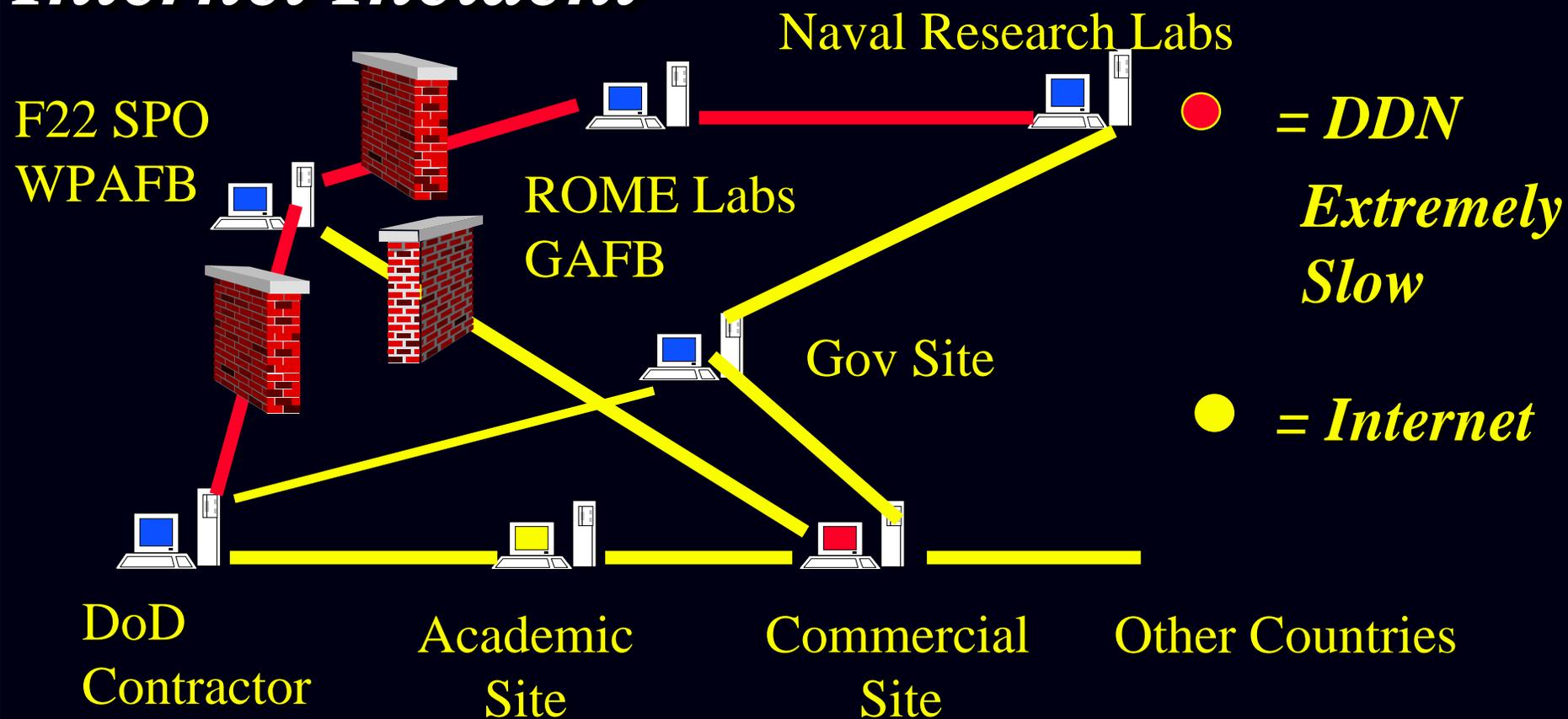
WEBSTER'S Ninth New Collegiate Dictionary



Defense-Wide Information Assurance Program



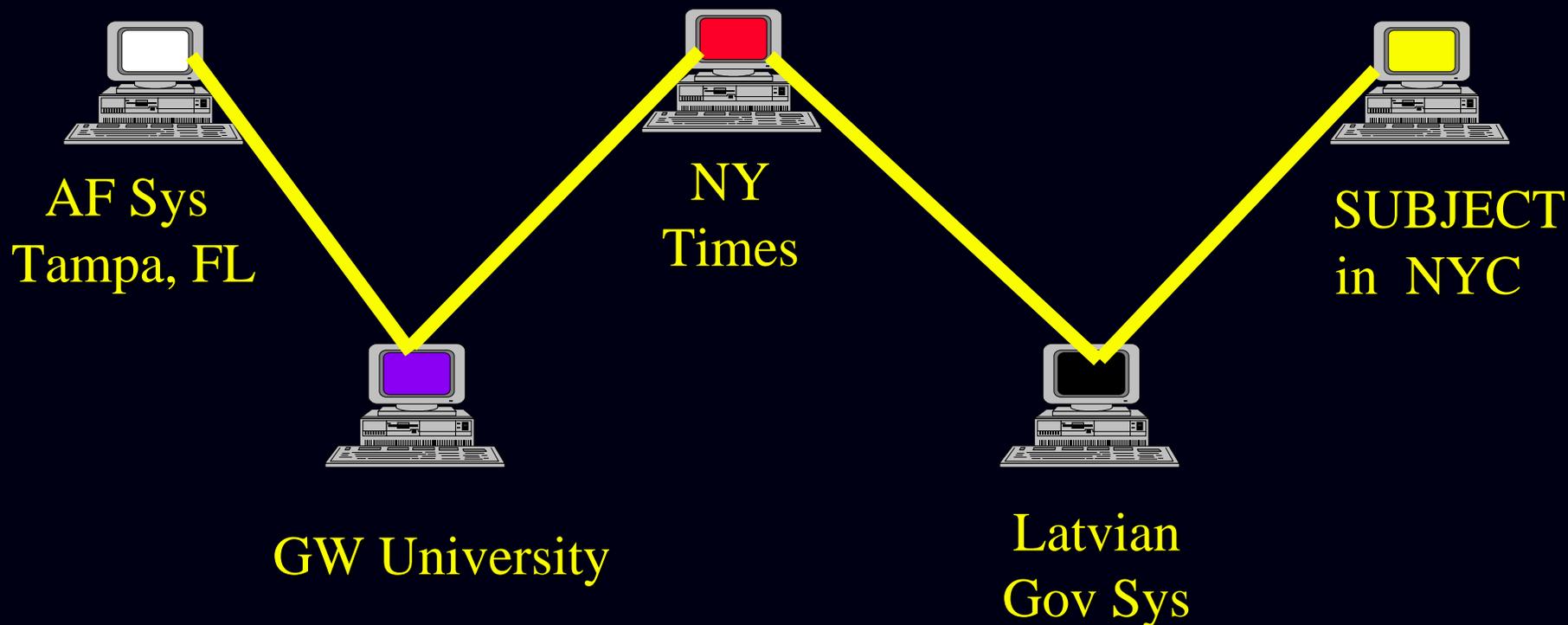
Internet Incident



Defense-Wide Information Assurance Program



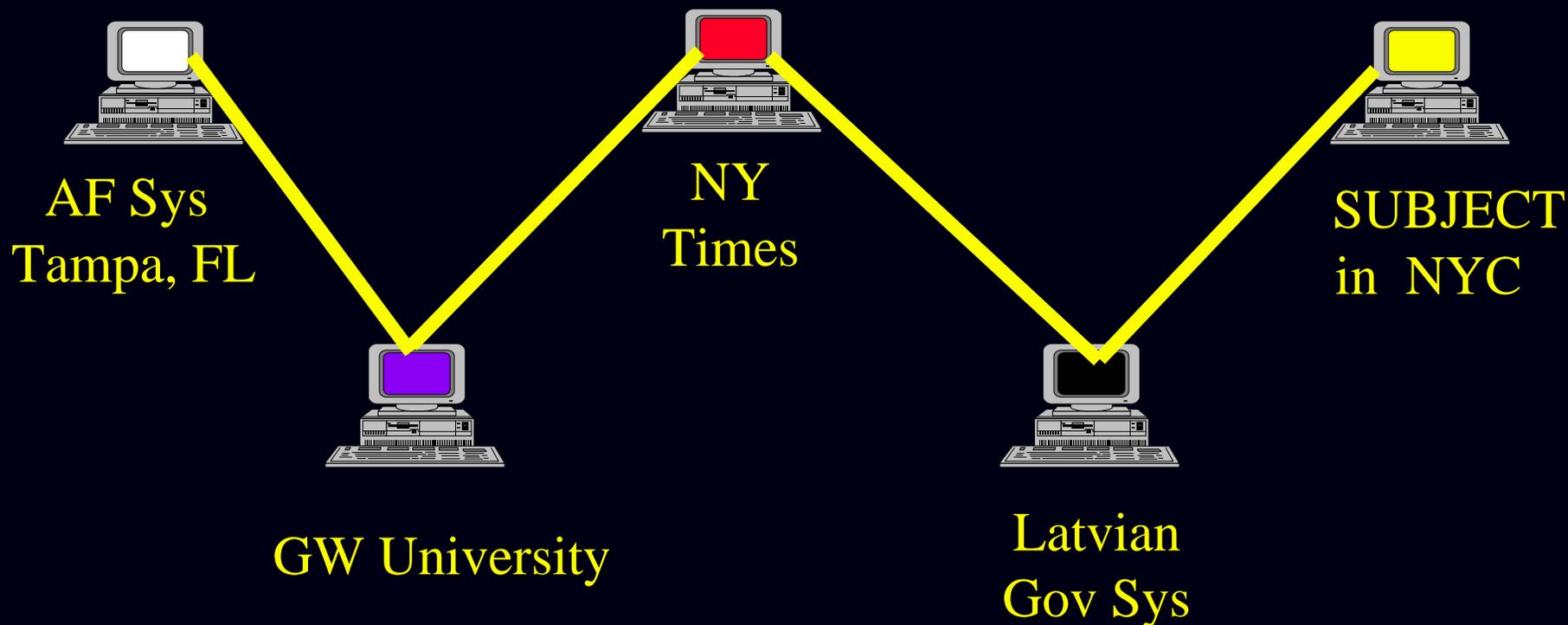
Hackers Loop & Weave to Prevent Detection & Identification



Defense-Wide Information Assurance Program



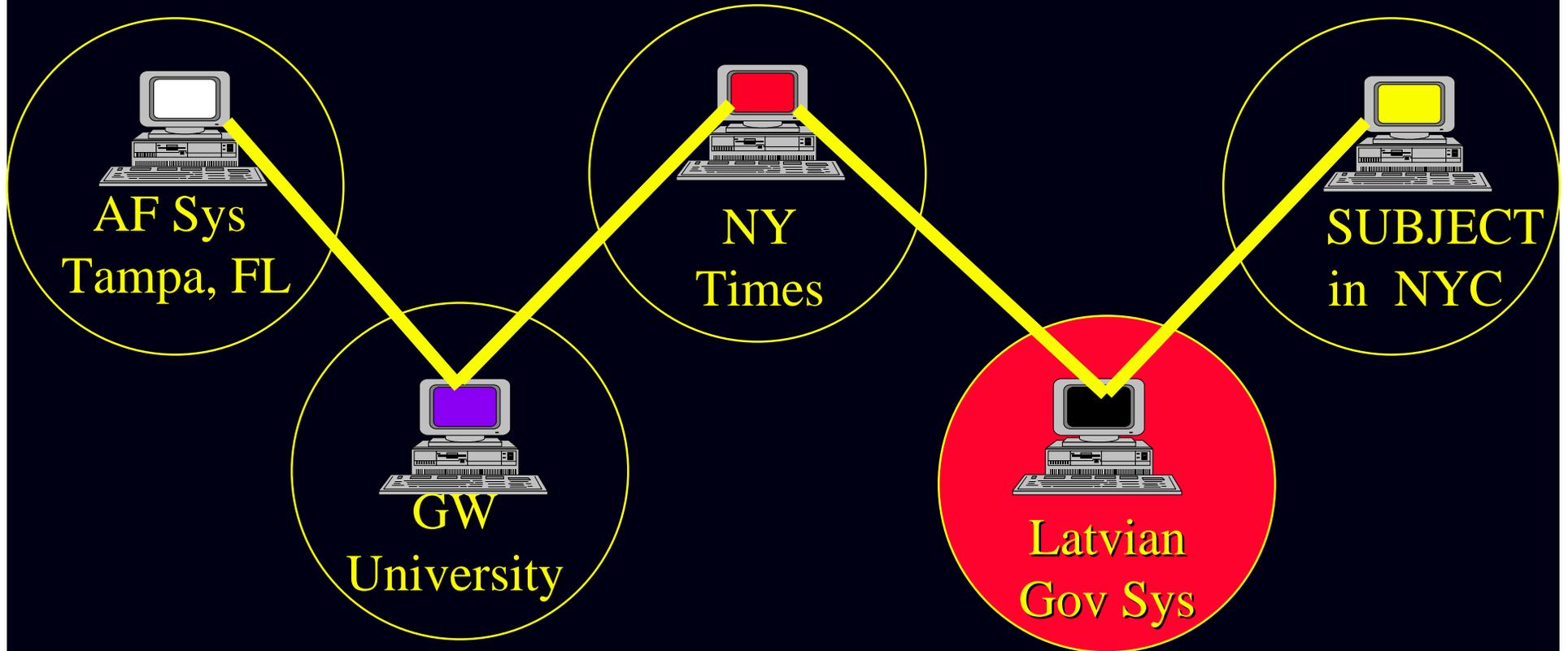
Traceback/Hackback



Defense-Wide Information Assurance Program



Court Jurisdiction Based on Geography

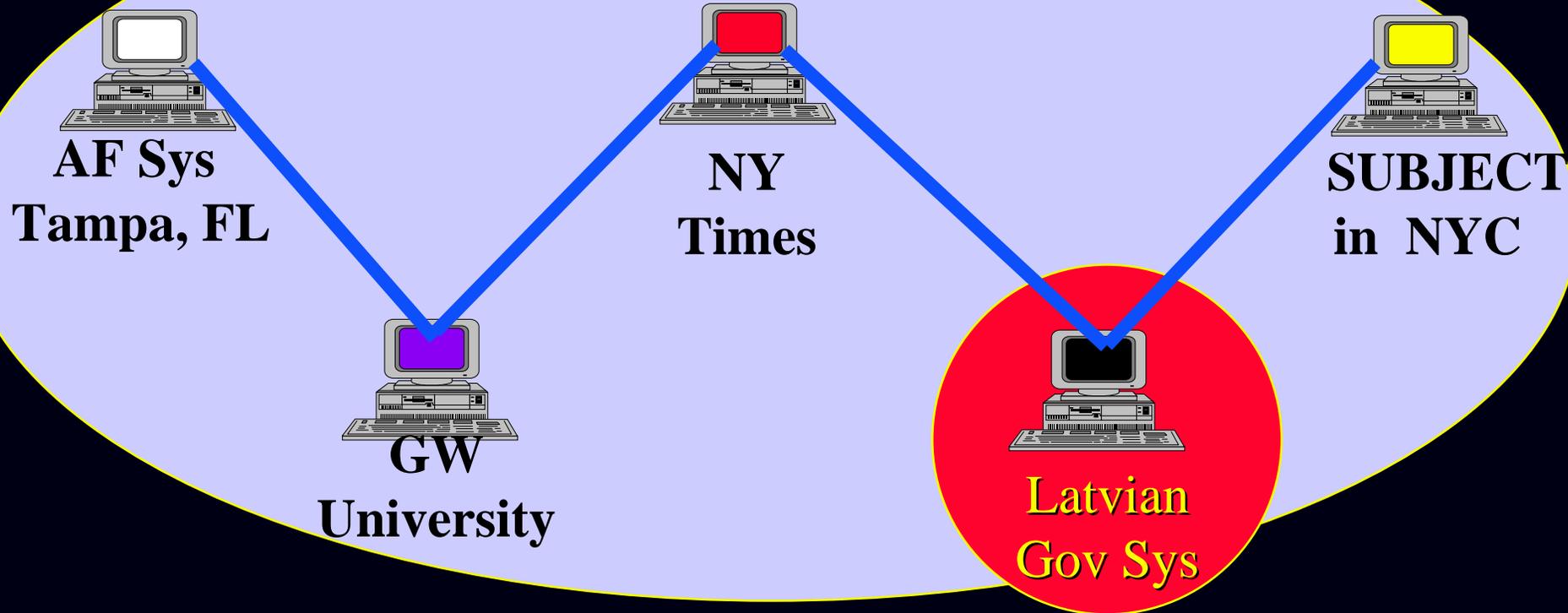


Defense-Wide Information Assurance Program



Cyber Court

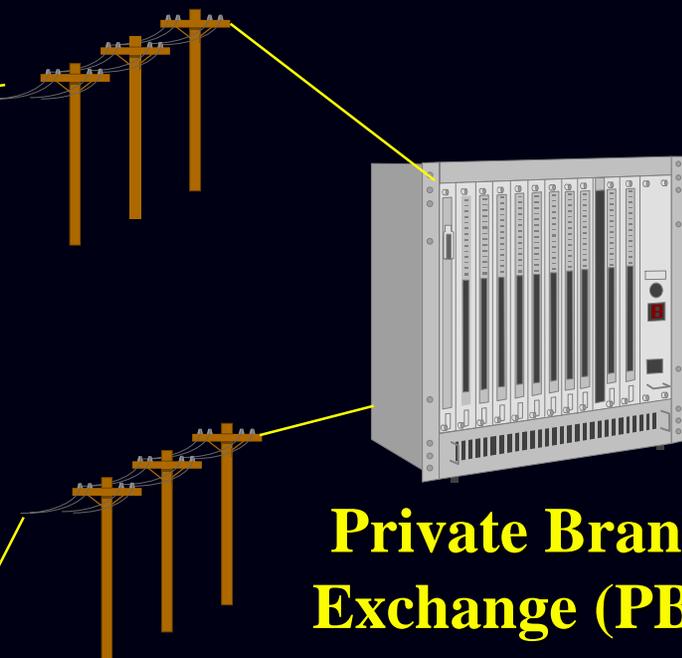
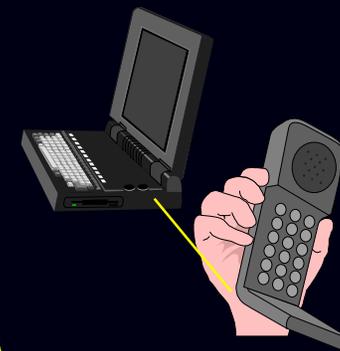
Jurisdiction for U.S. Cyberspace



Defense-Wide Information Assurance Program



Agent from Office



Private Branch Exchange (PBX)

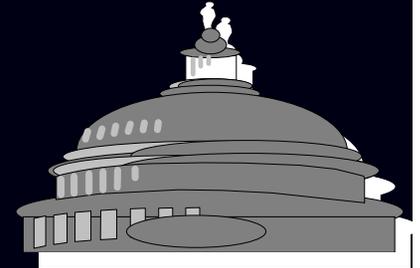


Phreaker Breaks into PBX, Installs Logical Wiretap

Internal & External Calls

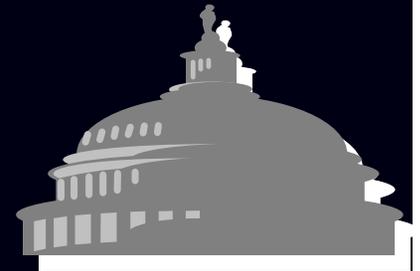
Defense-Wide Information Assurance Program

Manhattan
Cyber
Project



*U.S. Senate
Permanent Subcommittee
on Investigations*

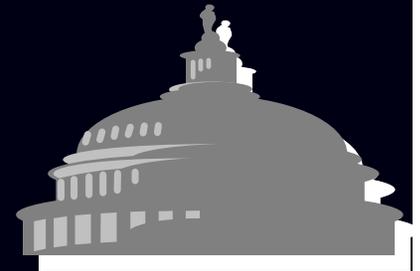
Defense-Wide Information Assurance Program



Subcommittee Hearings

- *Chaired by Senator Sam Nunn, GA*
- *Investigate the Threat to the National Information Infrastructure from a Cyberspace Attack (Jan-Aug 96)*

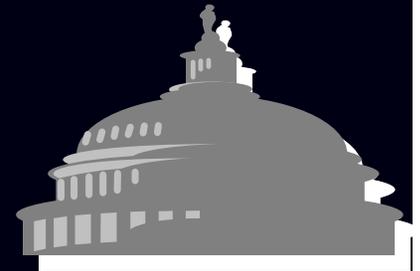
Defense-Wide Information Assurance Program



Subcommittee Hearings - Cyberspace Security

- Staff Interviewed > 200*
 - U.S. & International*
 - Government Leaders*
 - Computer Security Experts*
 - Law Enforcement Agencies*
 - Private Sector*

Defense-Wide Information Assurance Program



Subcommittee Hearings - Cyberspace Security

- Set of 4 Hearings (22 May, 5 Jun, 25 Jun, 16 Jul 96)

- Witnesses

- Dir CIA

- Dep Sec Def

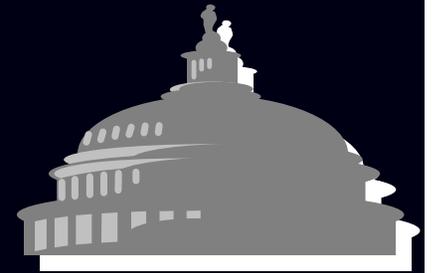
- Dep Attorney General

- Senators Kyl & Leahy

- Computer Security Experts

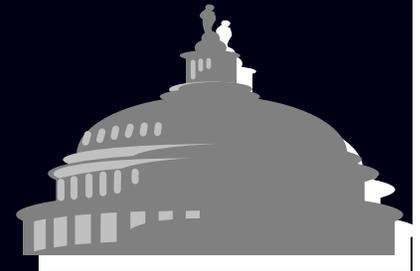
- Subcommittee Staff

Defense-Wide Information Assurance Program



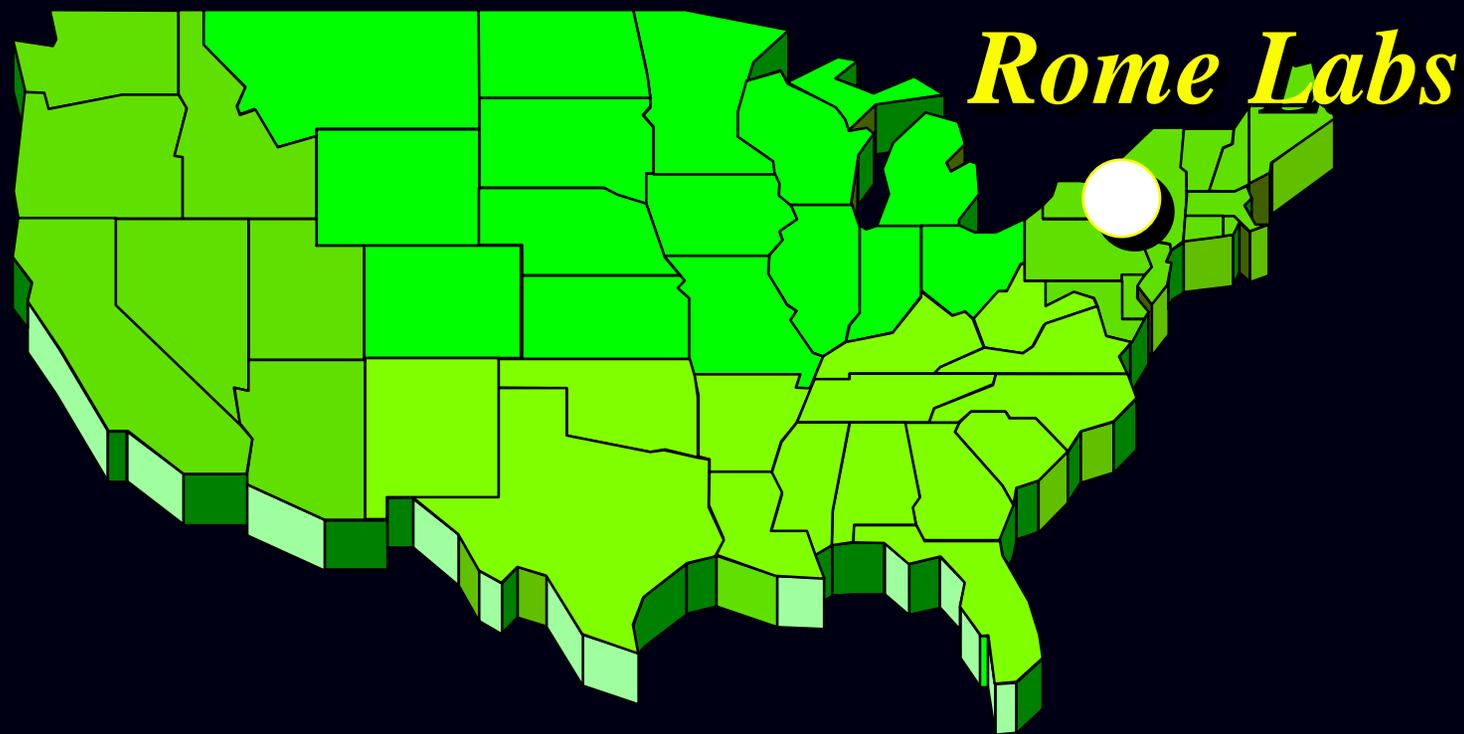
Hanover Hacker Case - 1986

- *Only Documented Computer Espionage Case*
- *OSI & FBI*
- *Five Hackers Levied by Soviet KGB*
 - *Drug & Financial Problems*
- *Best Seller “The Cuckoo’s Egg”*

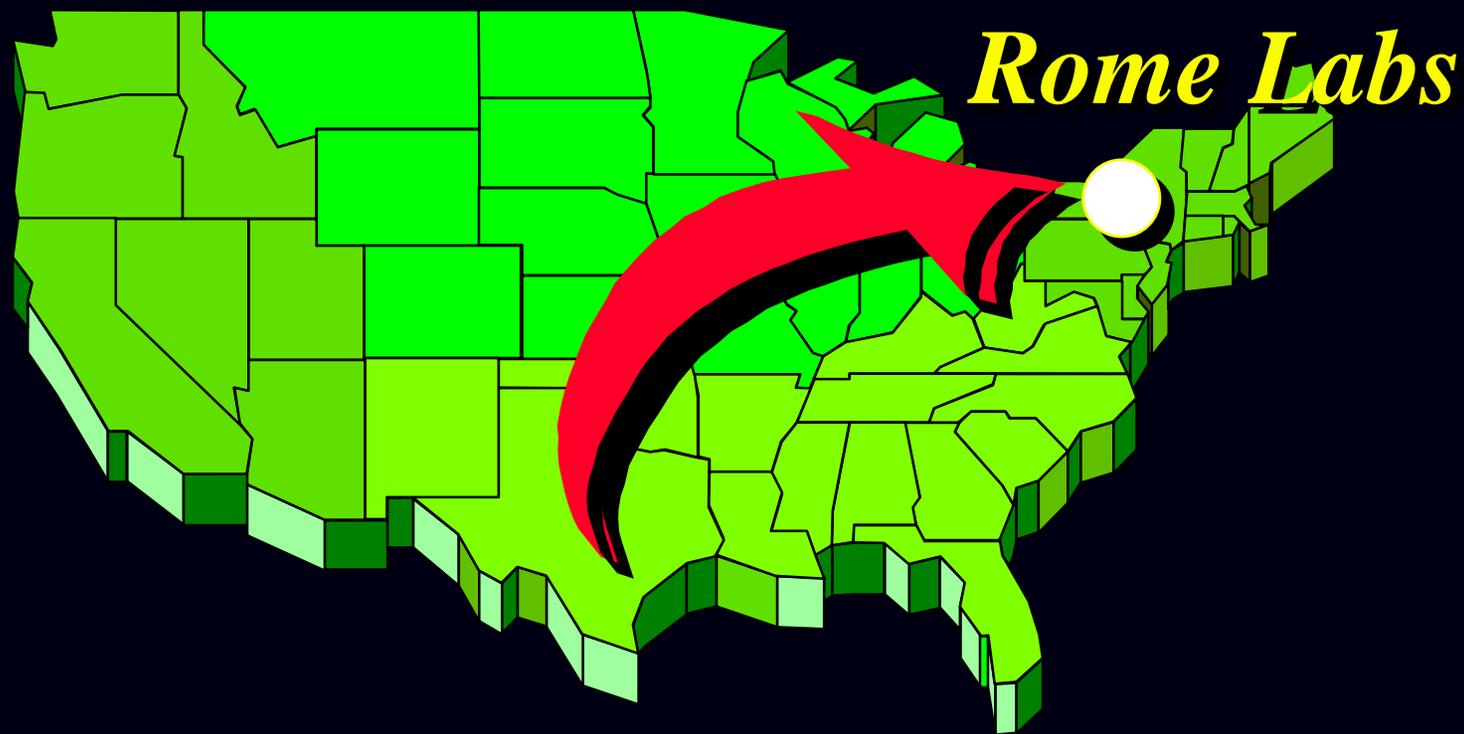


Mar - May 1994
Rome Air Development
Center
Griffiss AFB,
New York

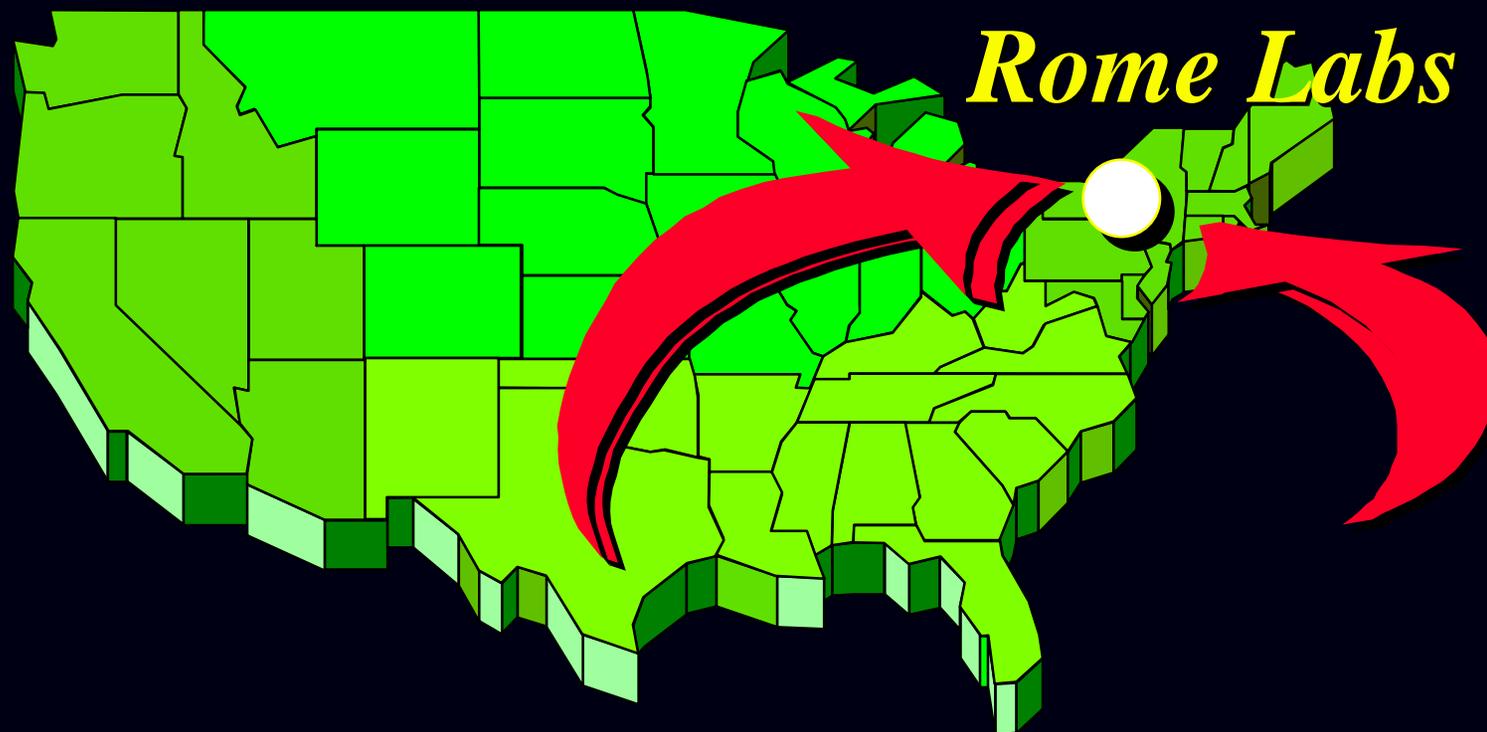
Defense-Wide Information Assurance Program



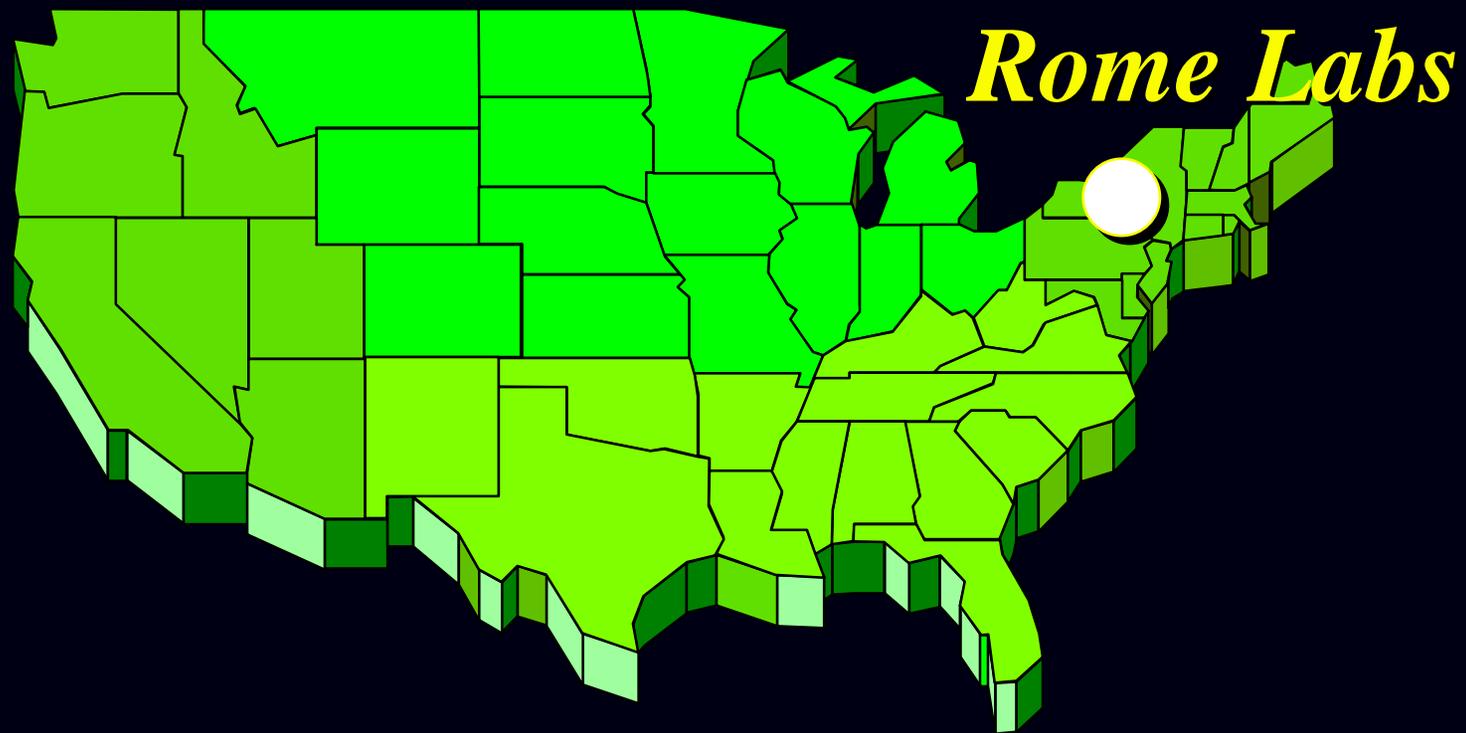
Rome Labs Discovers Sniffers



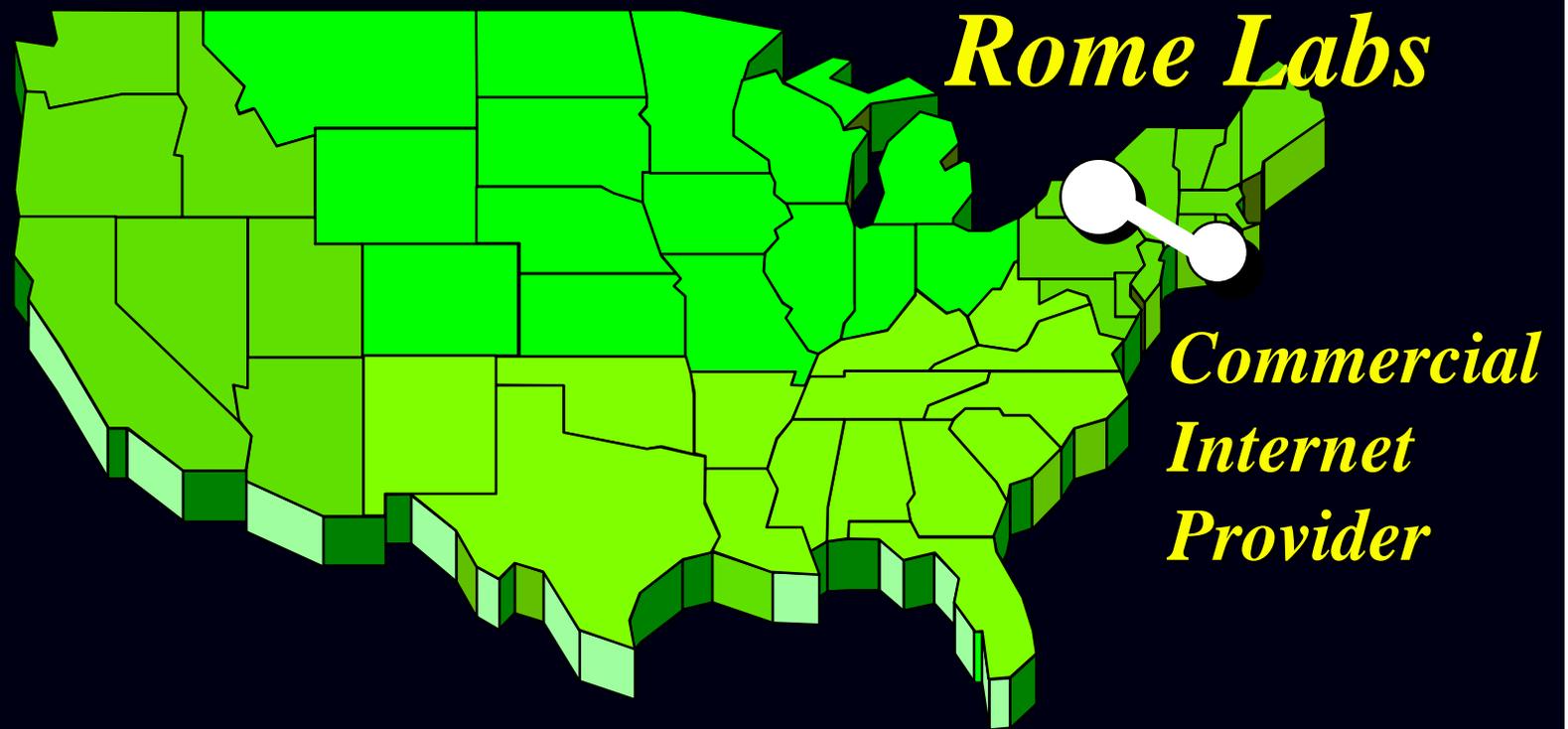
*AFCERT Deployed Teams
from Kelly AFB*



*AFOSI Deployed
Agents from Andrews AFB,*

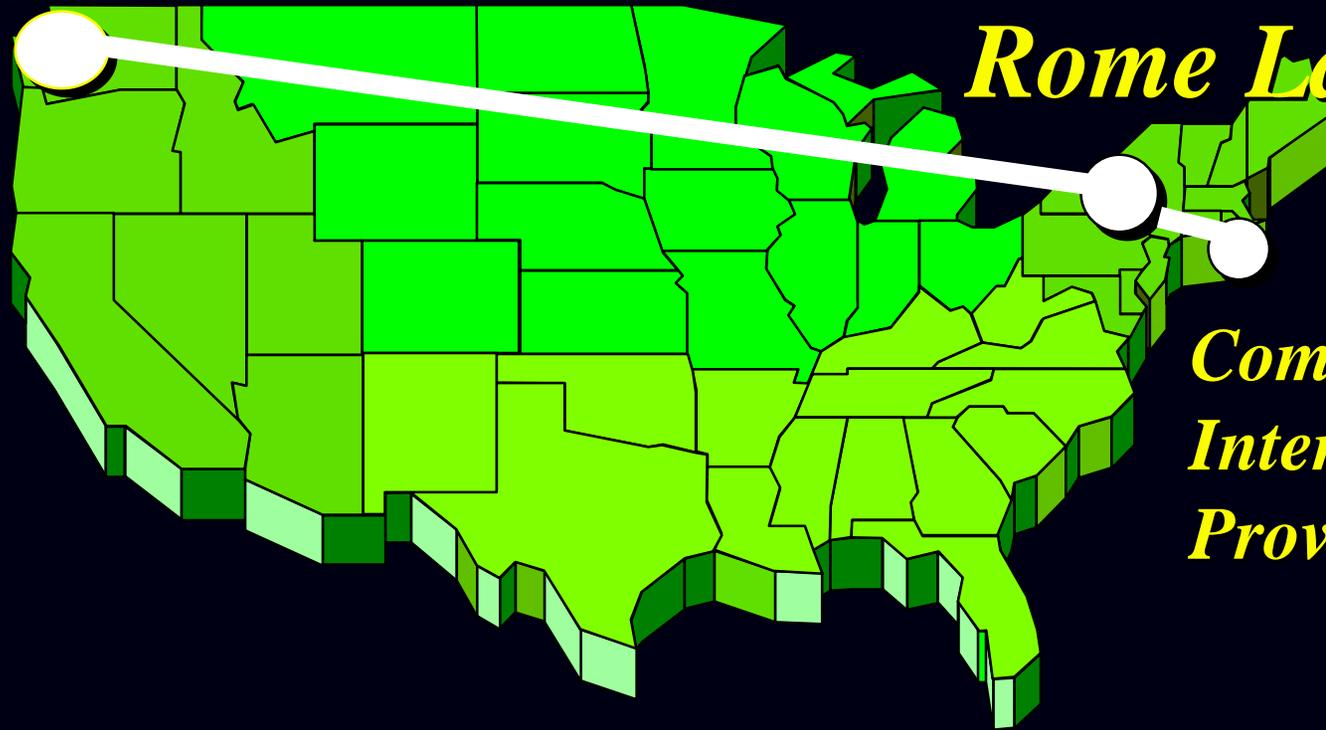


*Investigative Team Assessed Situation
Briefed Commander*



*Attacks Traced to Internet
Provider in New York*

*Commercial
Internet
Provider*

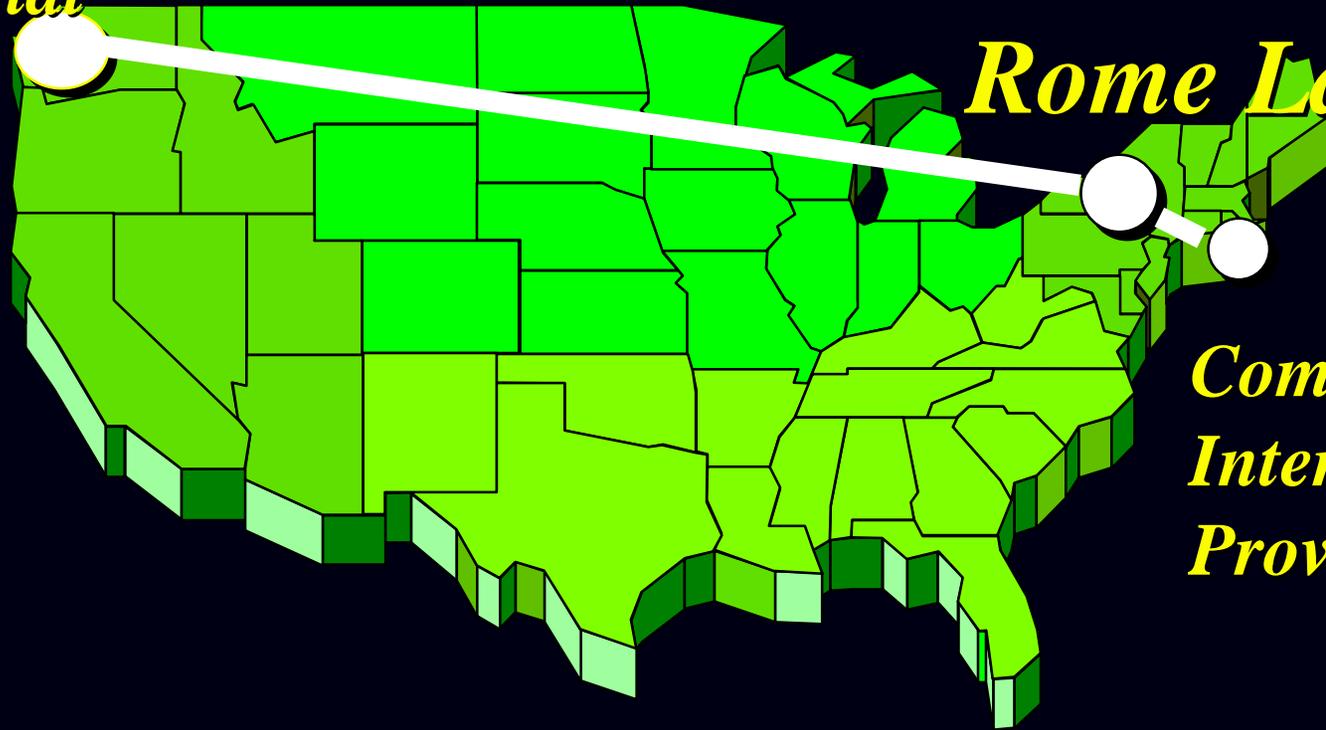


Rome Labs

*Commercial
Internet
Provider*

*Attacks Traced to Internet
Provider in Seattle, WA*

*Commercial
Internet
Provider*

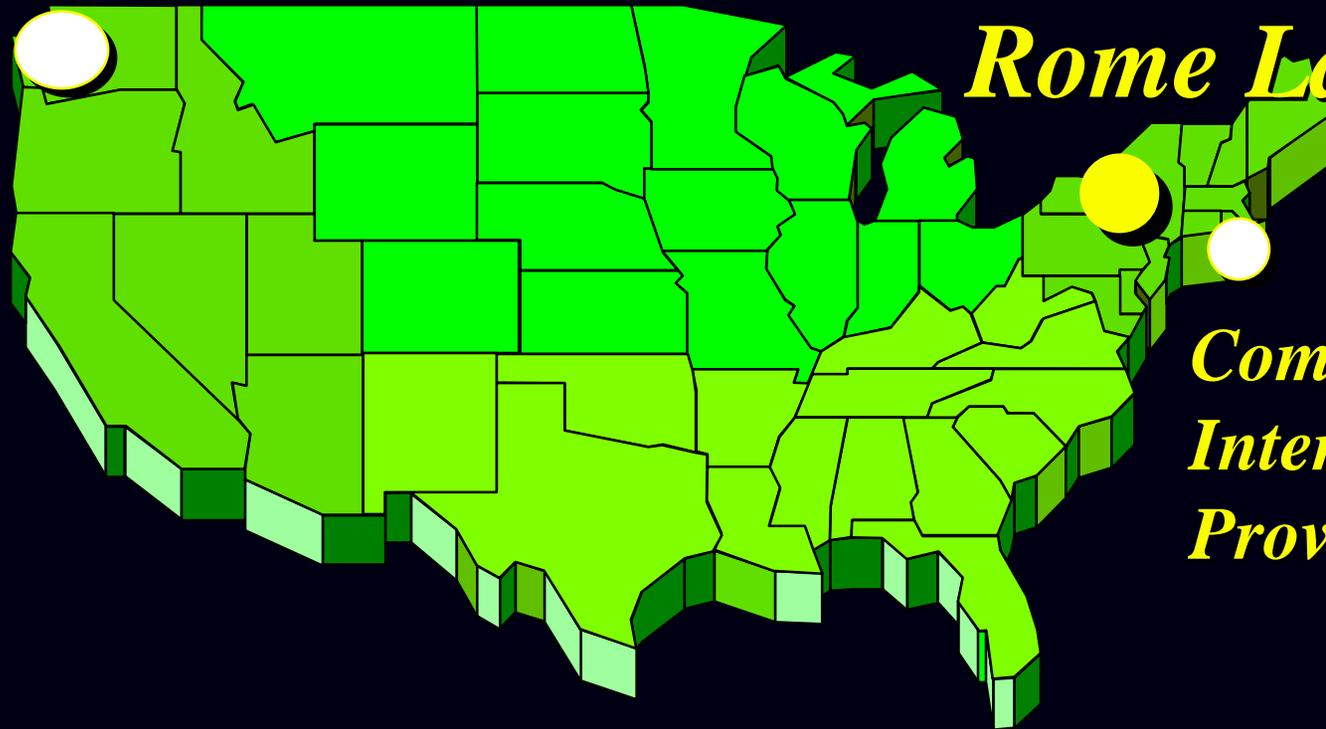


Rome Labs

*Commercial
Internet
Provider*

*Internet Path Deadend-Attackers
Using Phone Lines*

*Commercial
Internet
Provider*

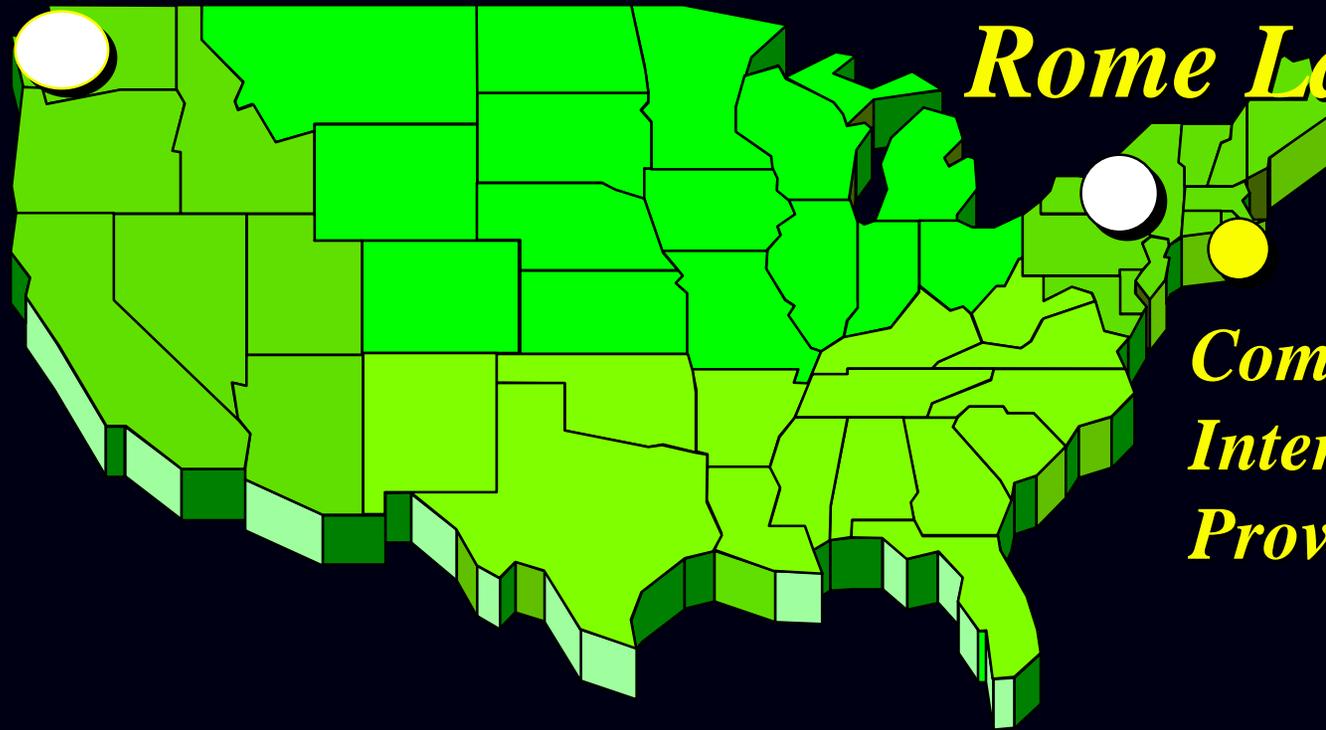


Rome Labs

*Commercial
Internet
Provider*

*Keystroke Monitoring
@ Rome Labs*

*Commercial
Internet
Provider*

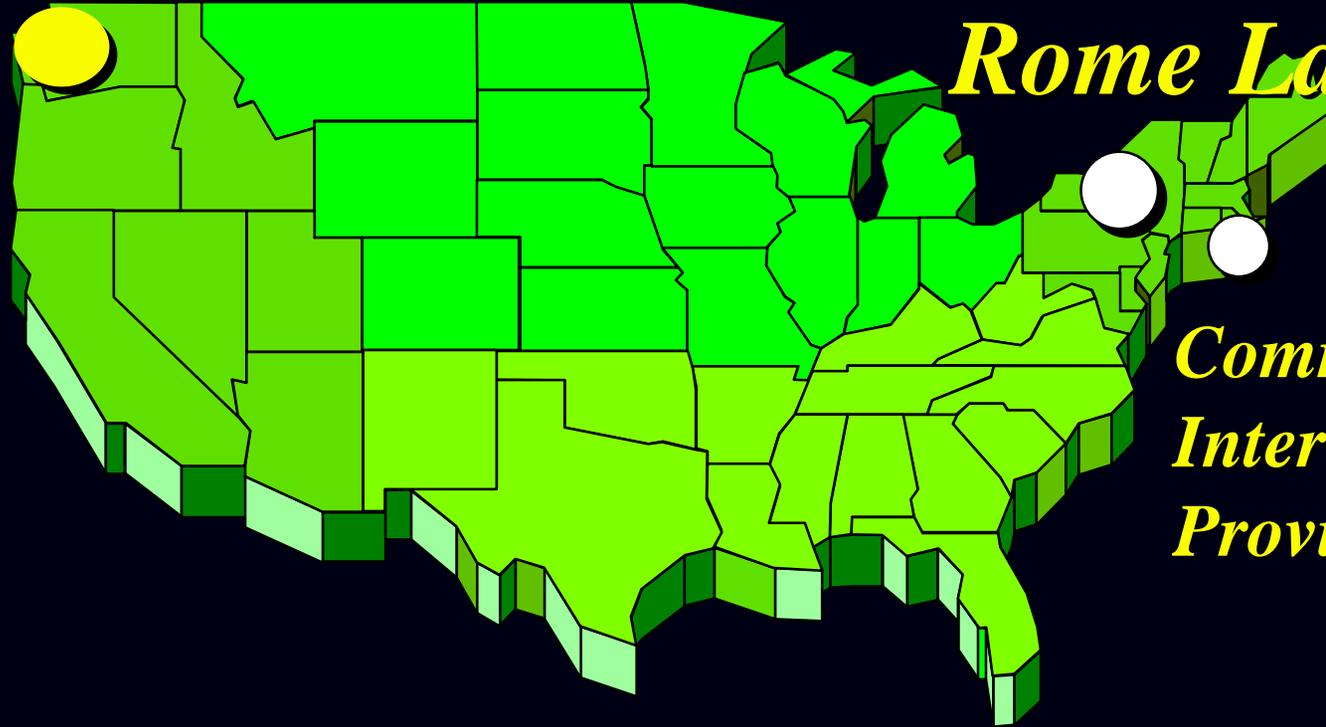


Rome Labs

*Commercial
Internet
Provider*

*Limited Context Monitoring
@ NY Internet Provider*

*Commercial
Internet
Provider*

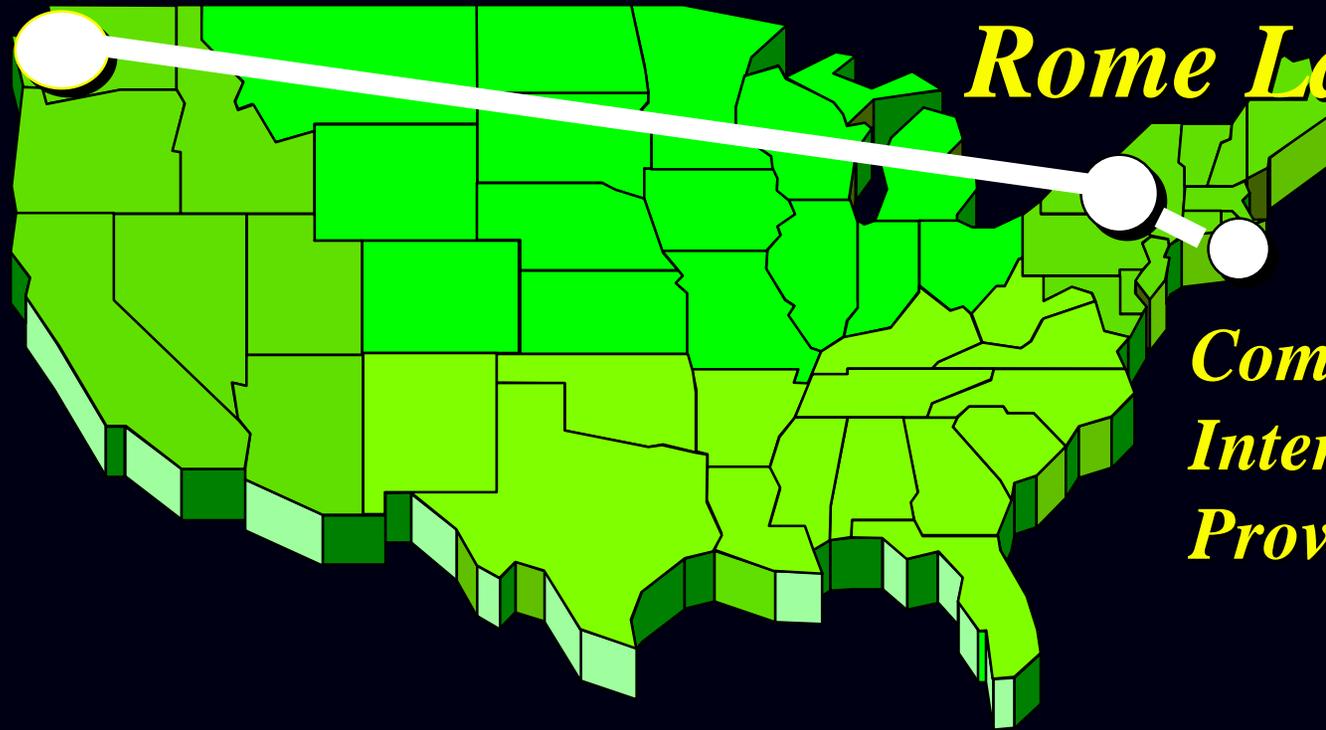


Rome Labs

*Commercial
Internet
Provider*

*Limited Context Monitoring @
WA Internet Provider*

*Commercial
Internet
Provider*

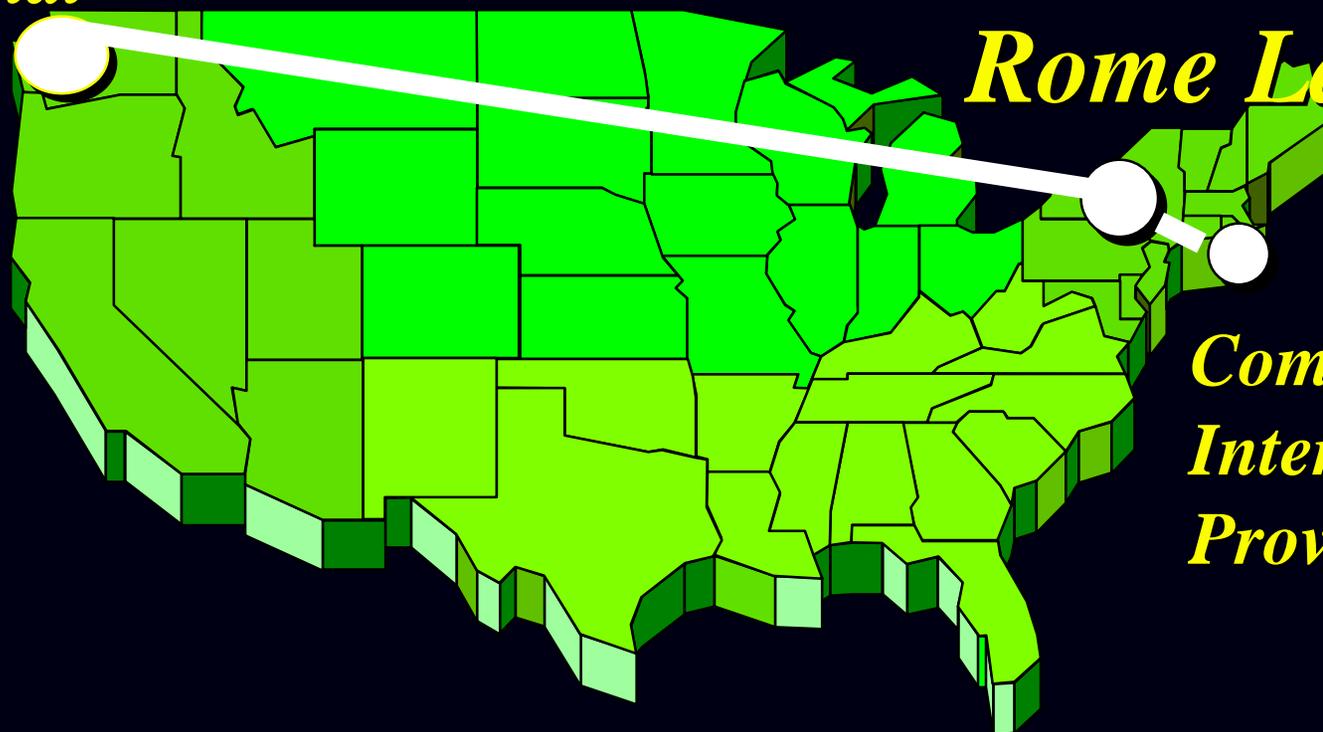


Rome Labs

*Commercial
Internet
Provider*

*Handles of Hackers were
Kuji & Datastream*

*Commercial
Internet
Provider*

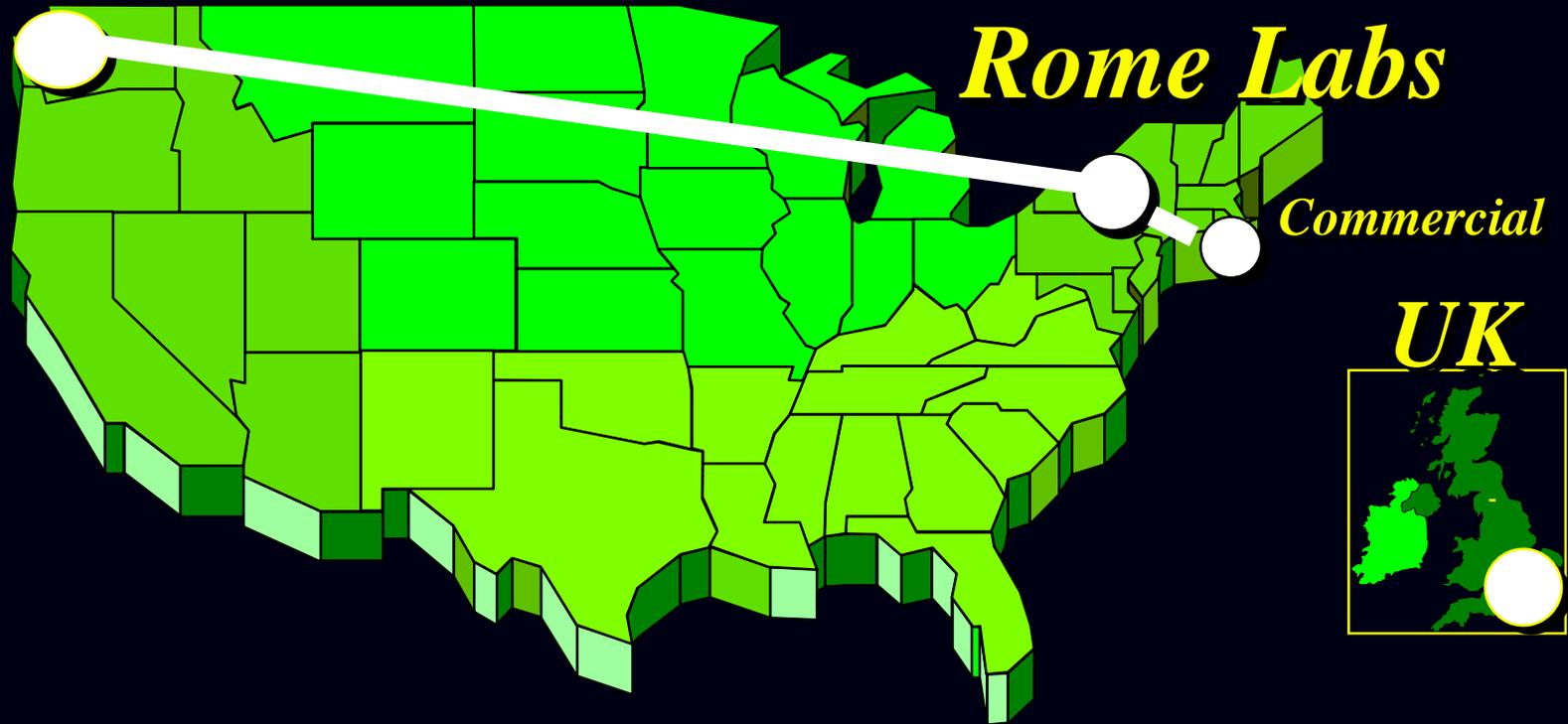


Rome Labs

*Commercial
Internet
Provider*

*Agents Requested
Help from Informants*

Commercial



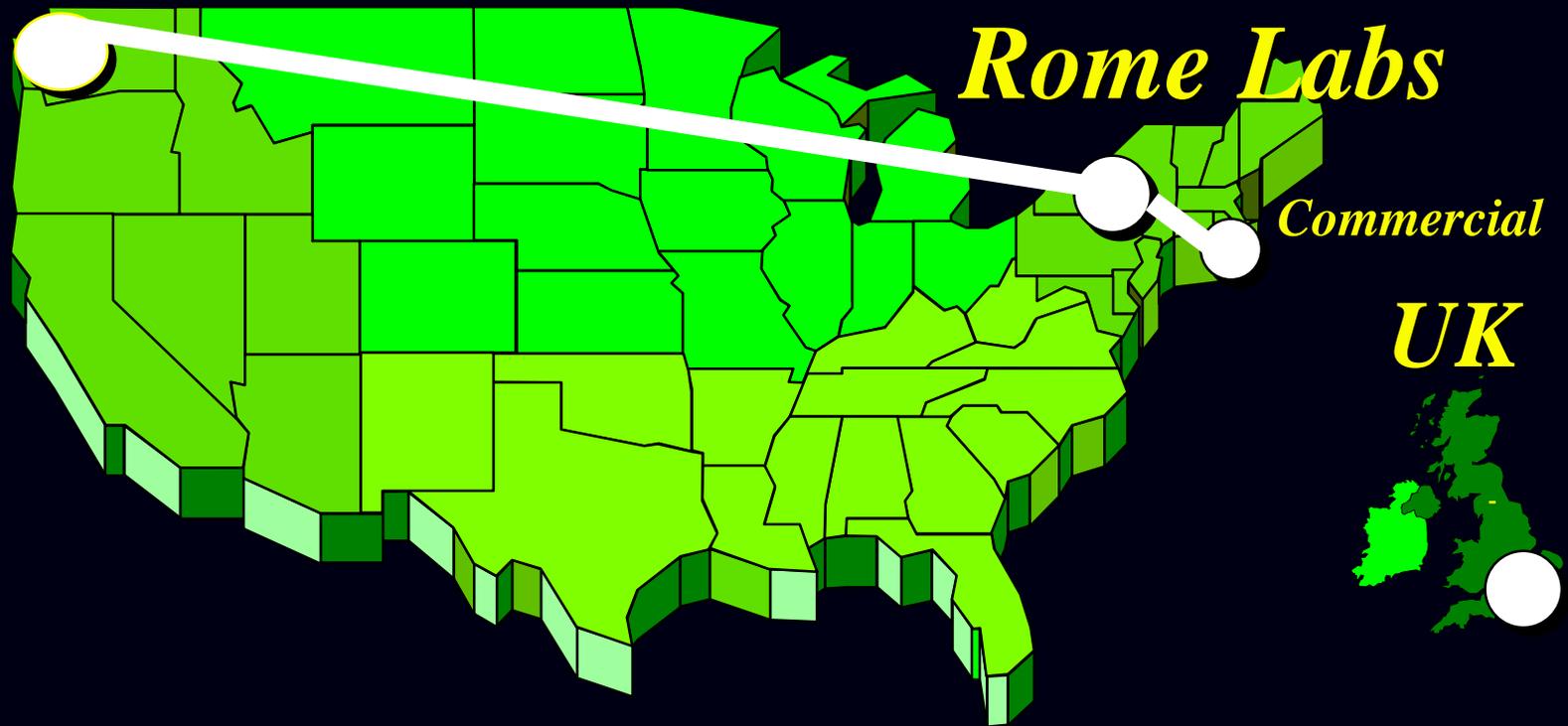
Rome Labs

Commercial

UK

*Informant Identifies
Hacker from UK*

Commercial



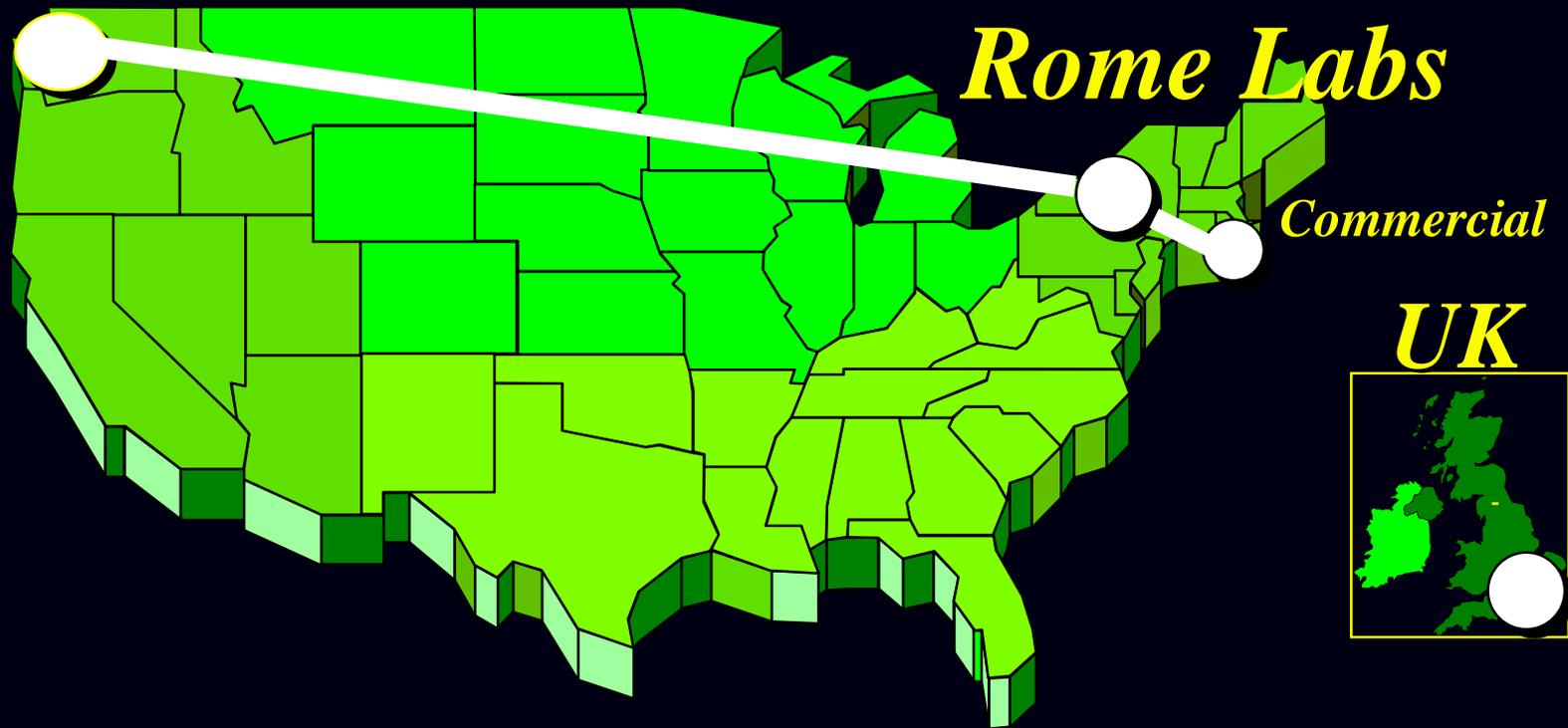
Rome Labs

Commercial

UK

*Hacks .MIL Sites Because
So Easy*

Commercial



Rome Labs

Commercial

UK

*Agents Call CCU Scotland
Yard. Pen Registers Up*

Commercial

Rome Labs

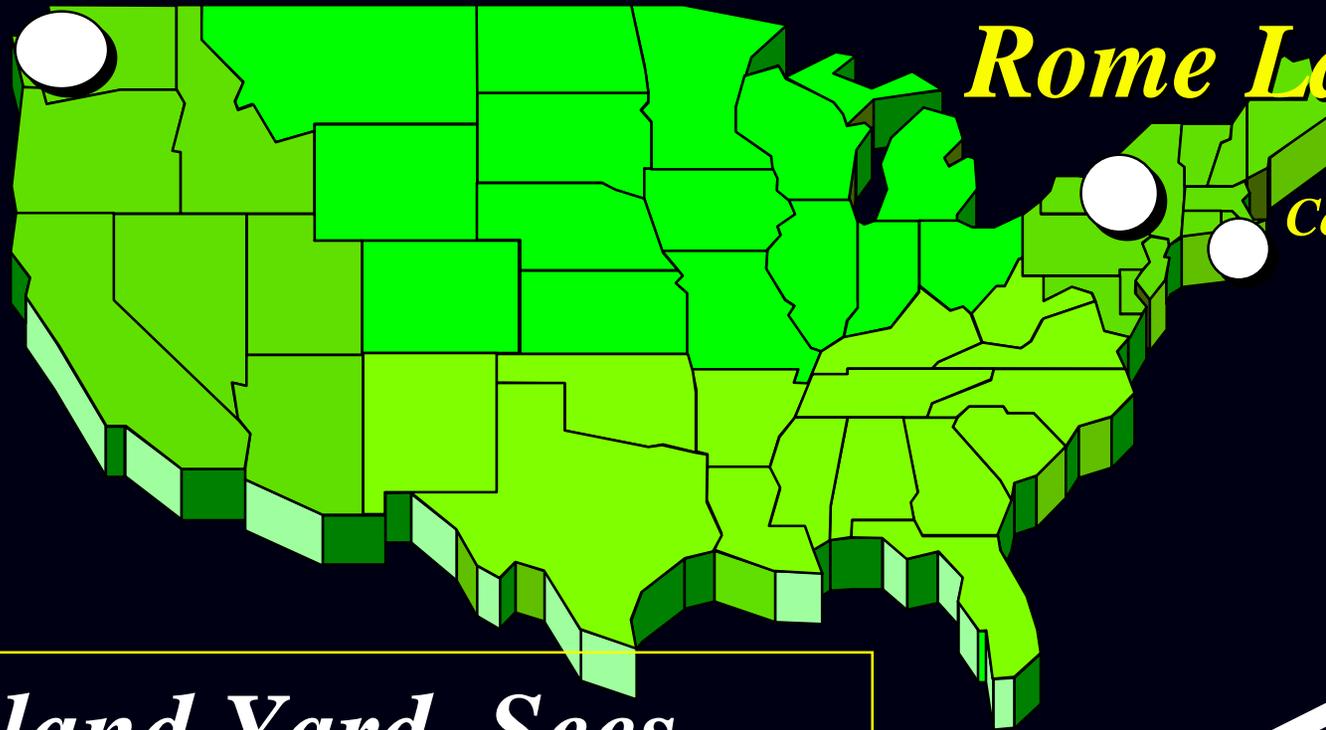
Commercial

UK

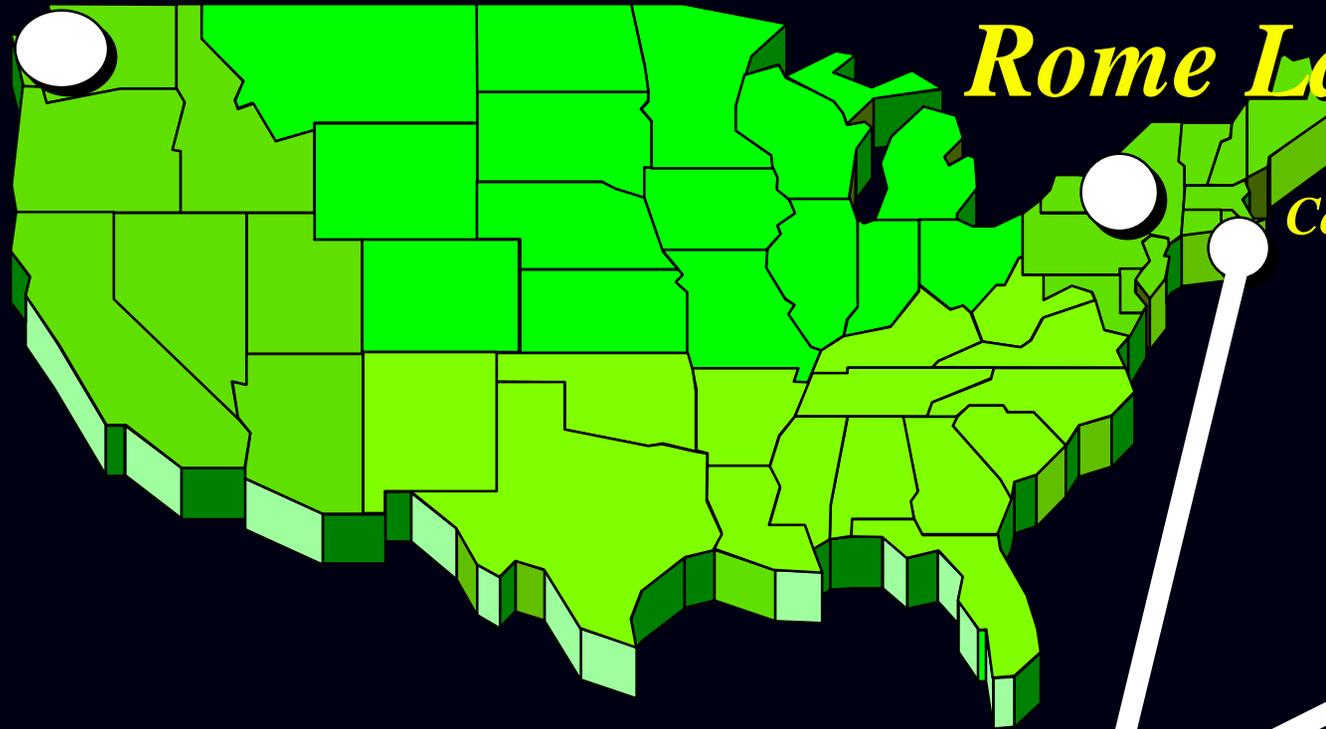


*Colombia
&
Chile*

*Scotland Yard Sees,
Phreaking thru South
America*



Commercial



Rome Labs

Commercial

UK



*Colombia
&
Chile*

*Phreaking thru South
America to New York*

Commercial

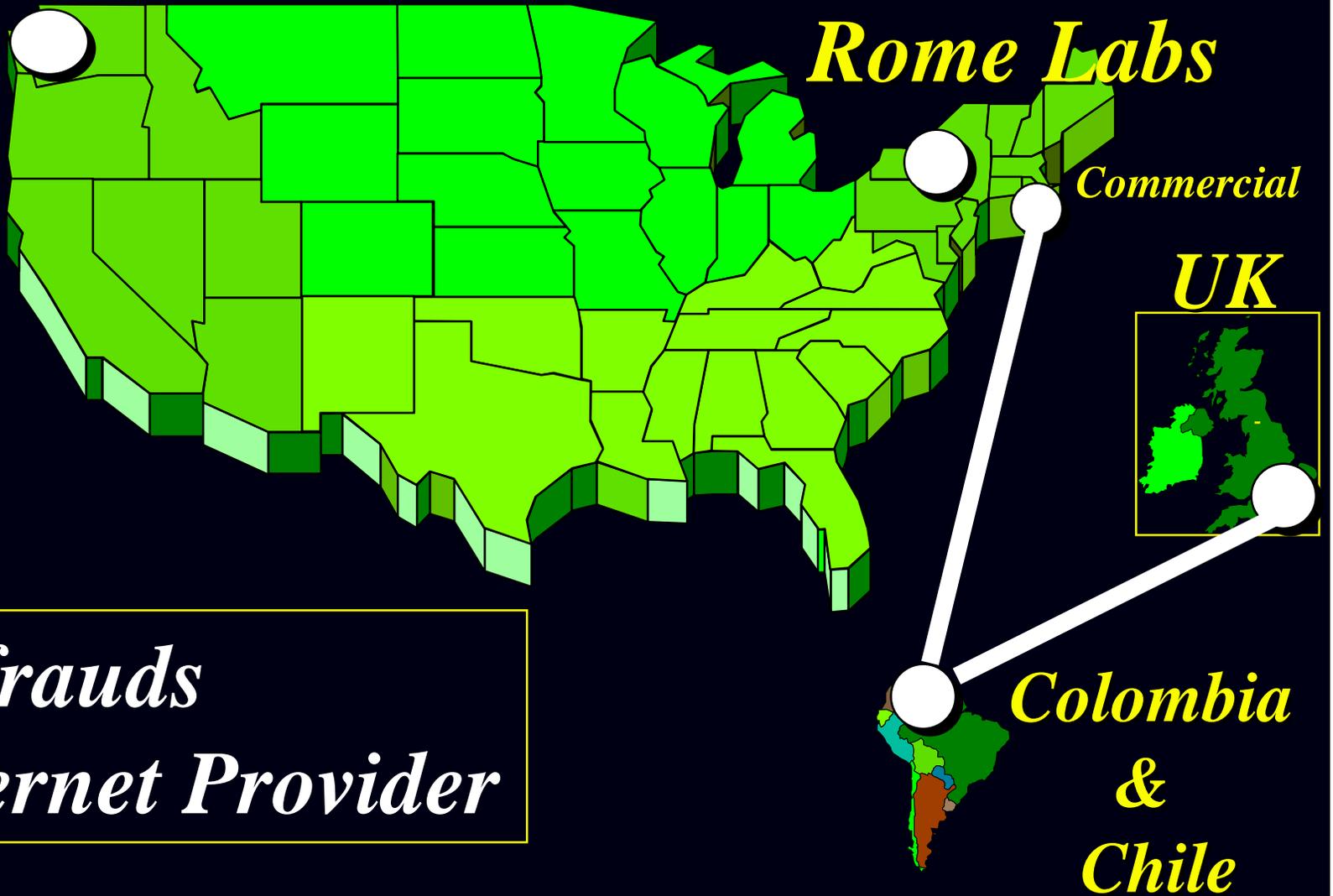
Rome Labs

Commercial

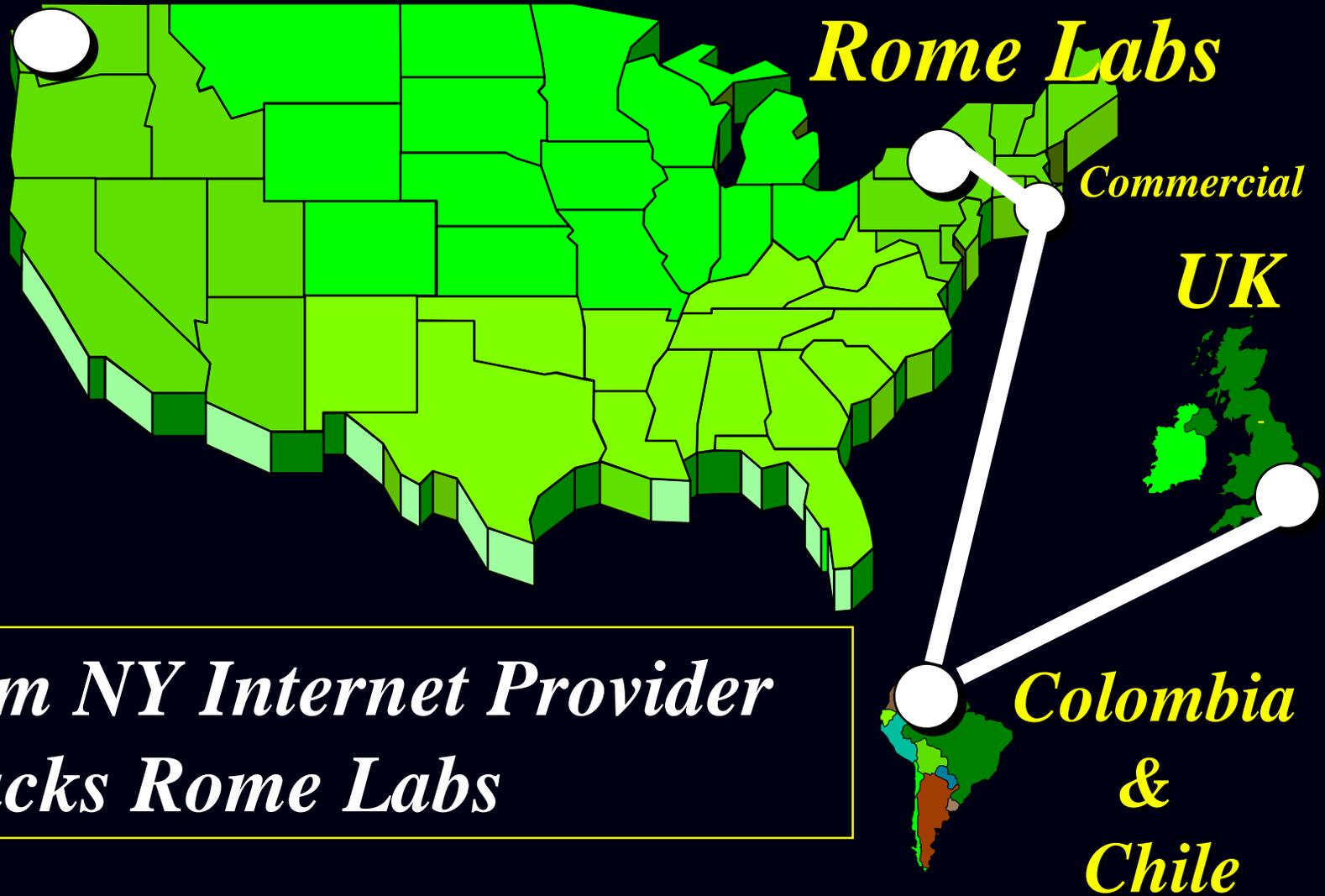
UK

*Defrauds
Internet Provider*

*Colombia
&
Chile*



Commercial



*From NY Internet Provider
Attacks Rome Labs*

Commercial

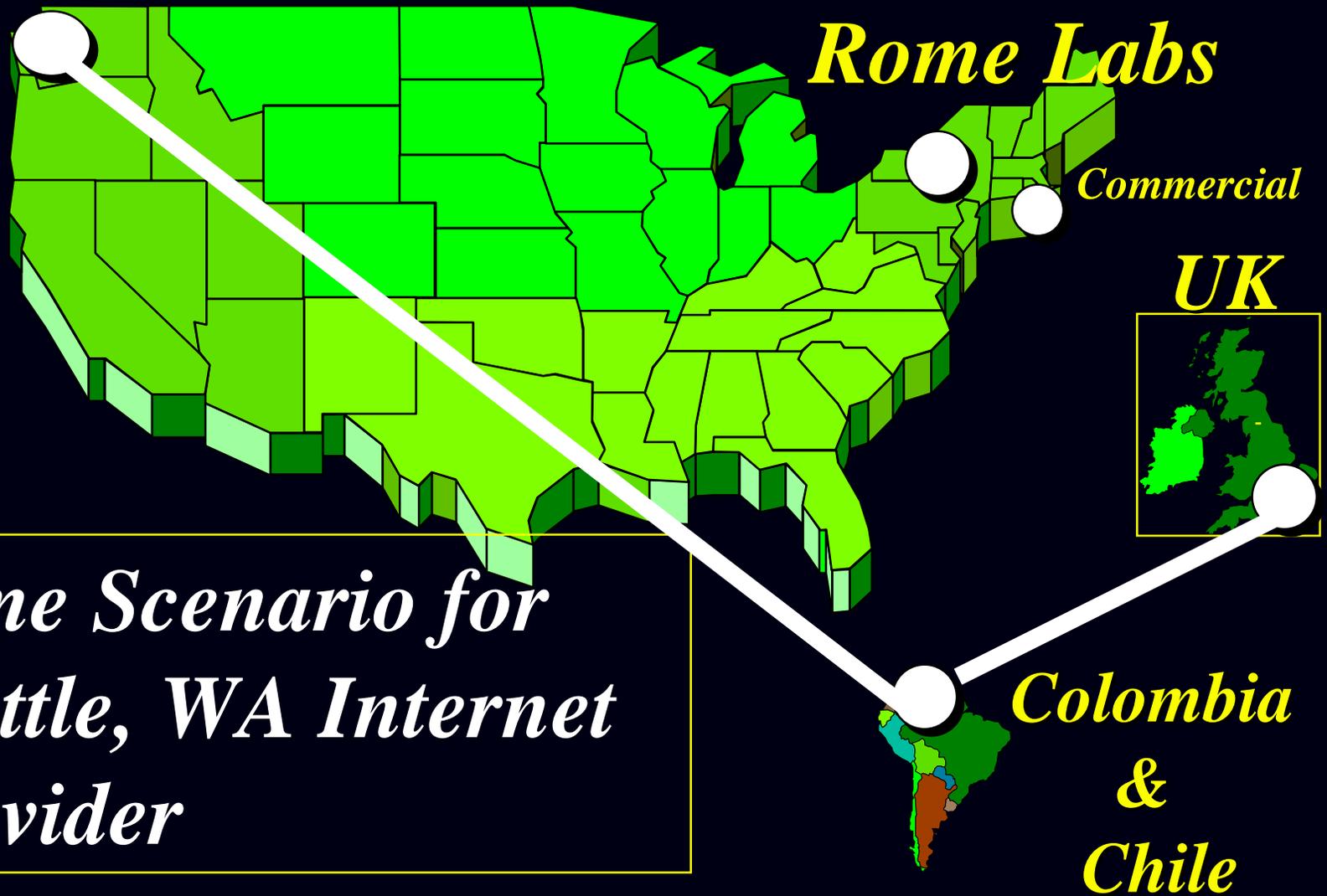
Rome Labs

Commercial

UK

*Same Scenario for
Seattle, WA Internet
Provider*

*Colombia
&
Chile*



Commercial

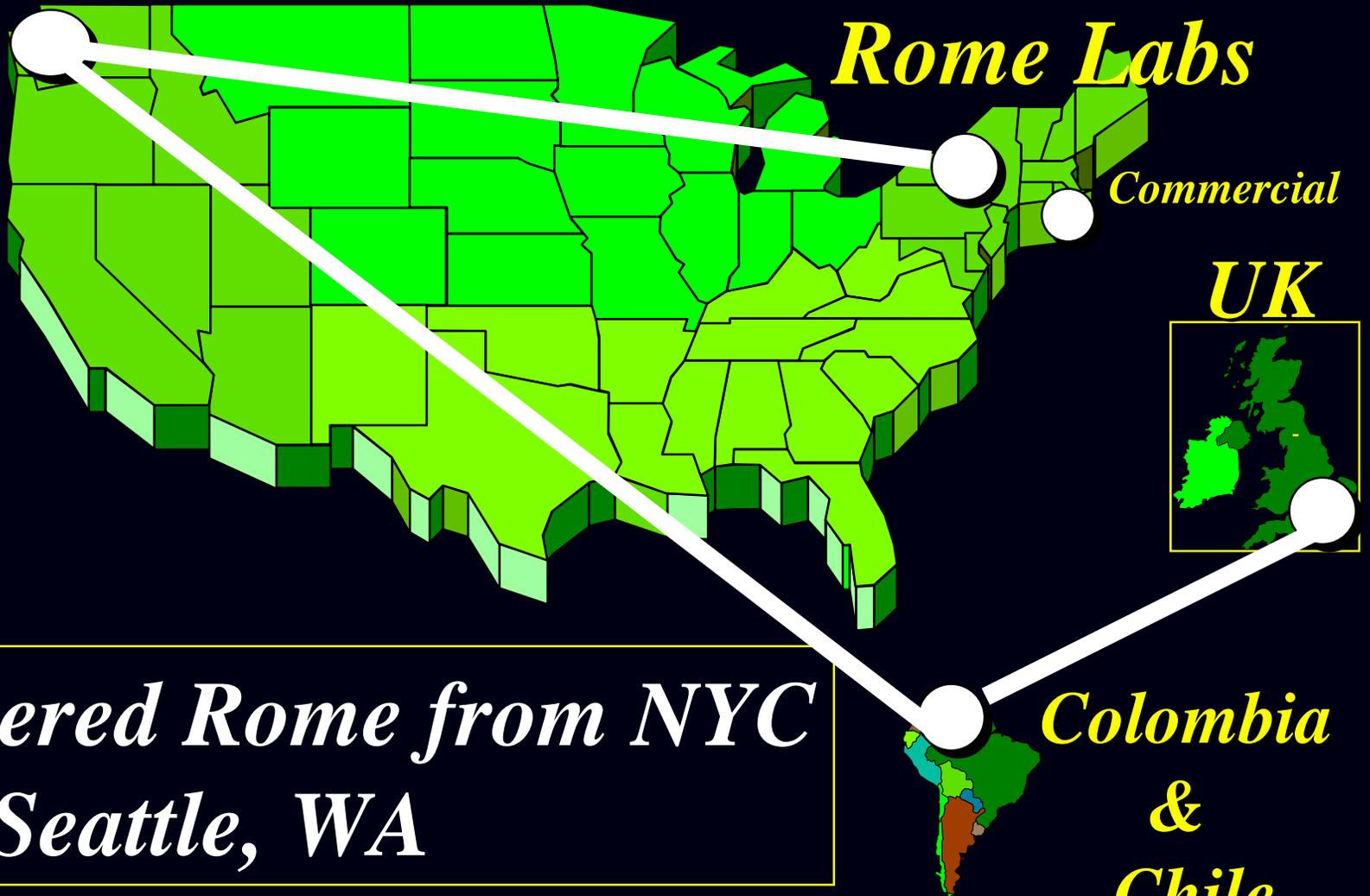
Rome Labs

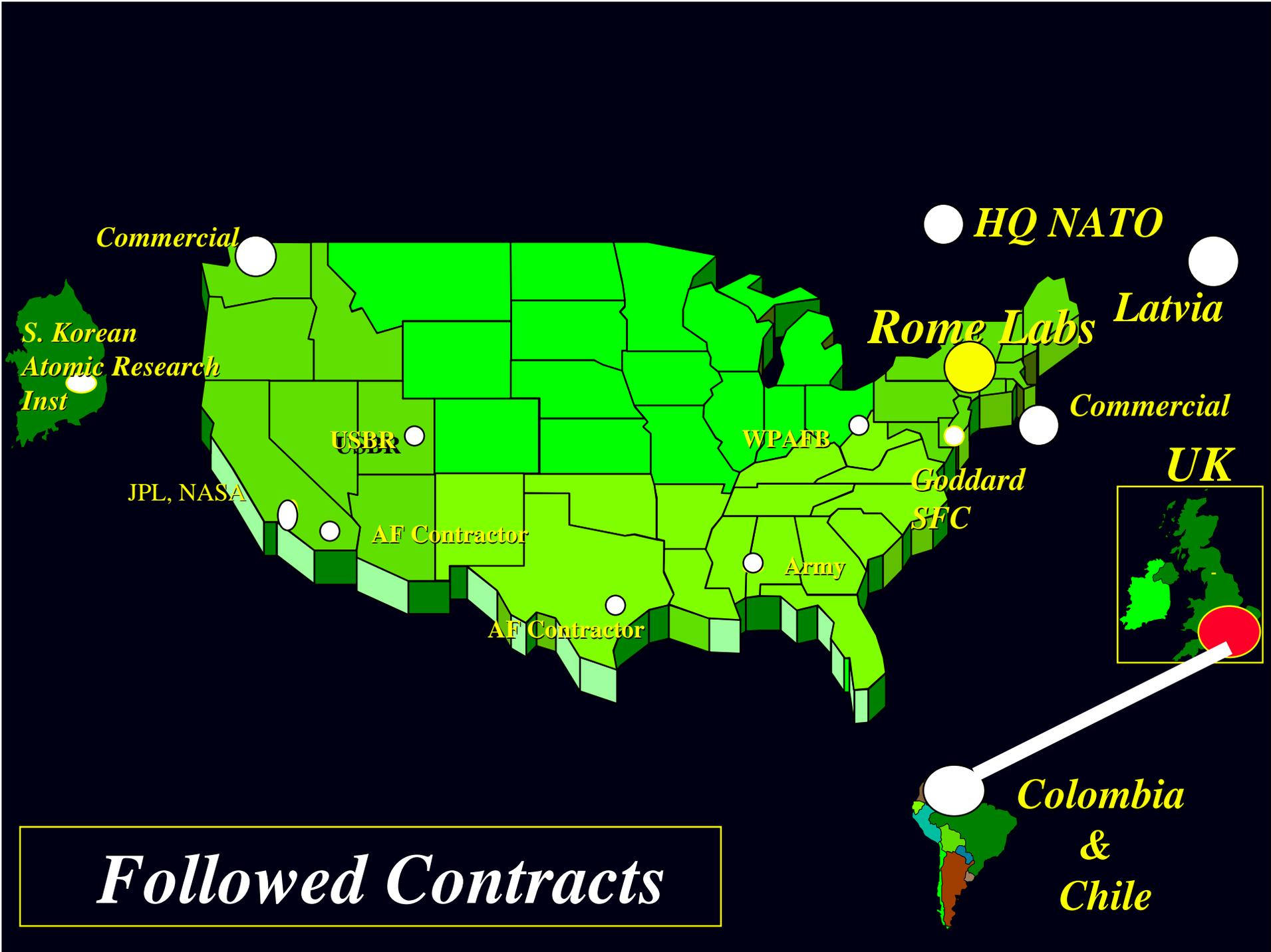
Commercial

UK

*Entered Rome from NYC
or, Seattle, WA*

*Colombia
&
Chile*





Commercial

*S. Korean
Atomic Research
Inst*

USBR

JPL, NASA

AF Contractor

AF Contractor

WPAFB

Army

*Goddard
SFC*

Rome Labs

HQ NATO

Latvia

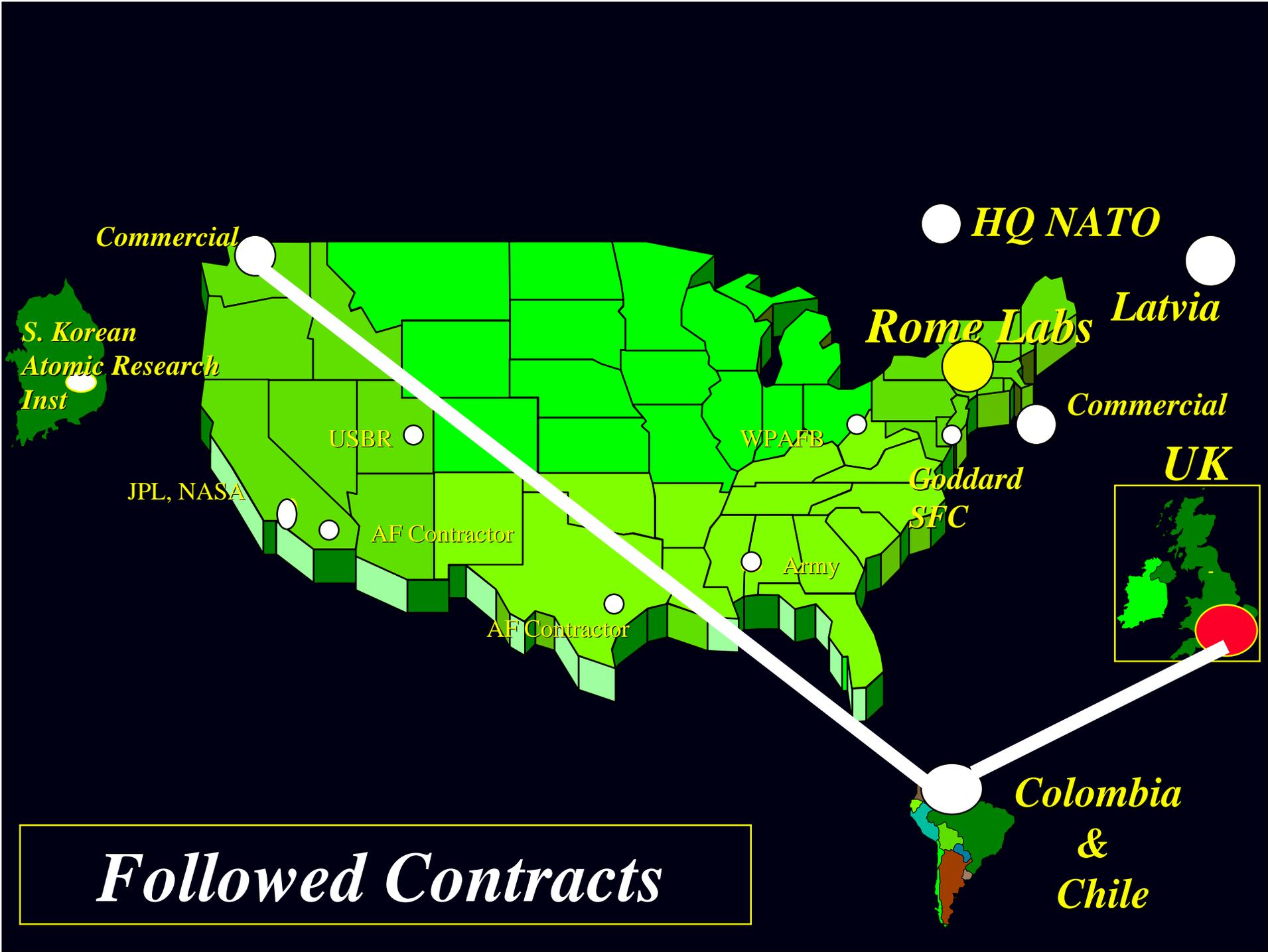
Commercial

UK

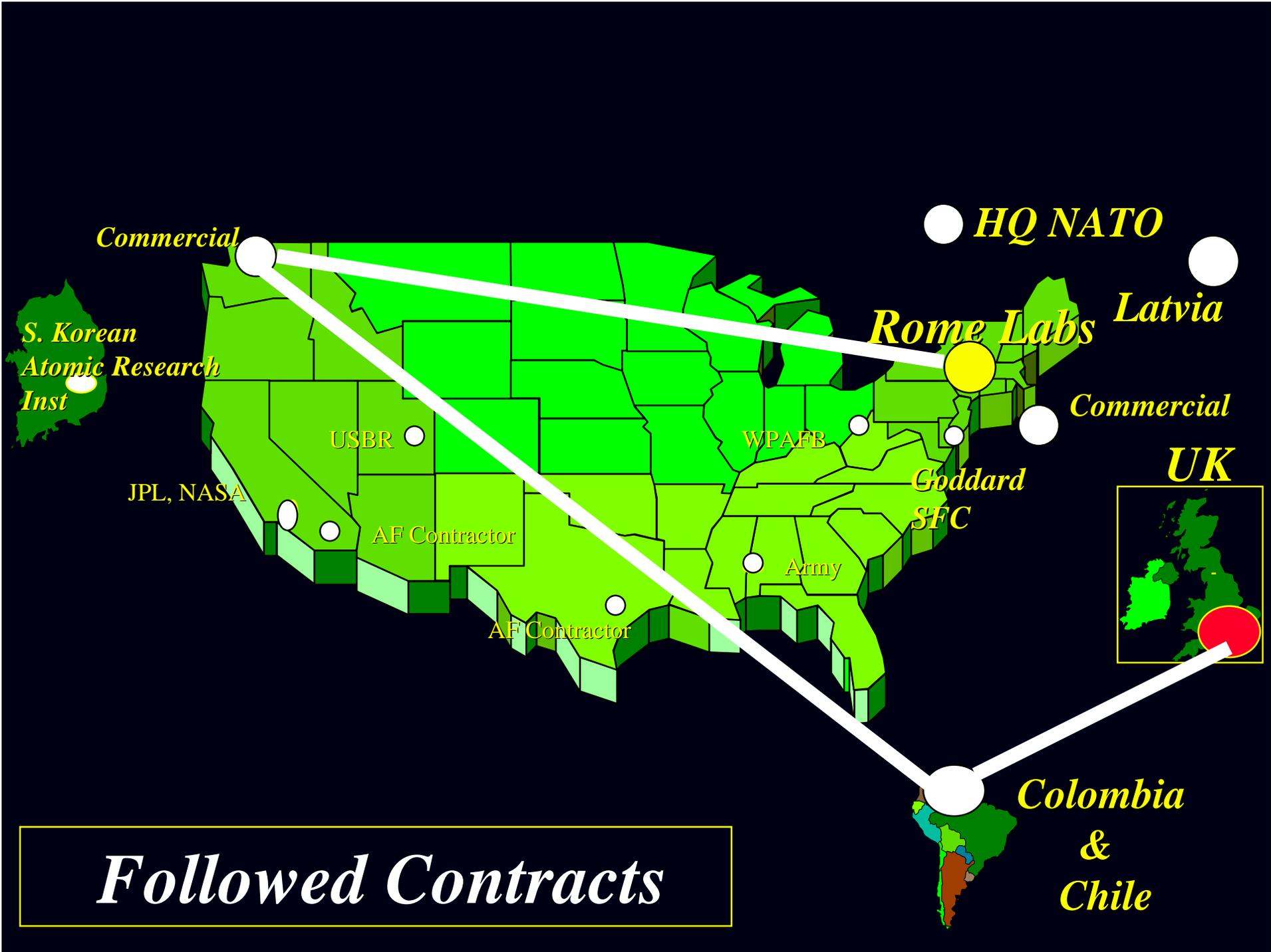


*Colombia
&
Chile*

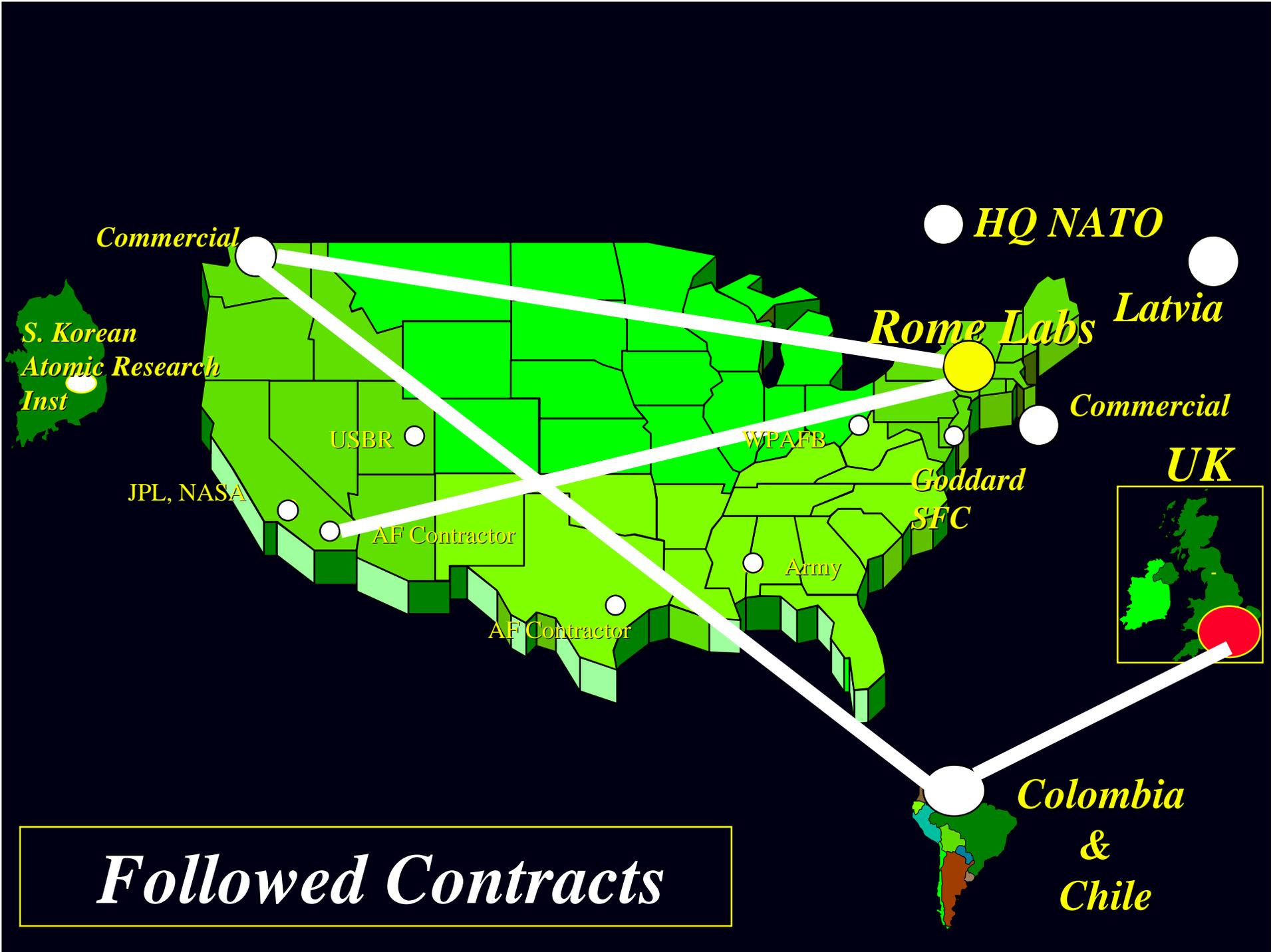
Followed Contracts

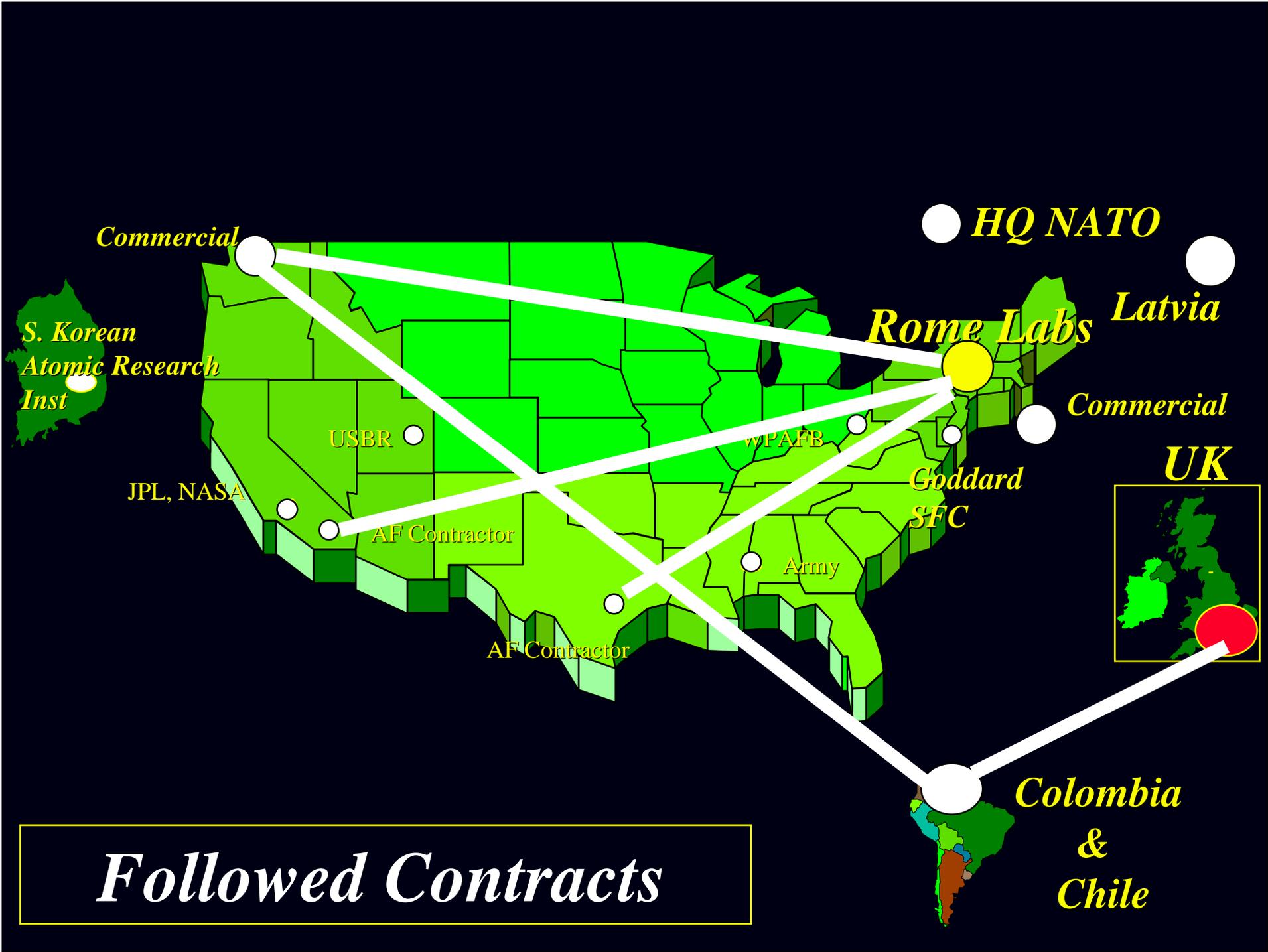


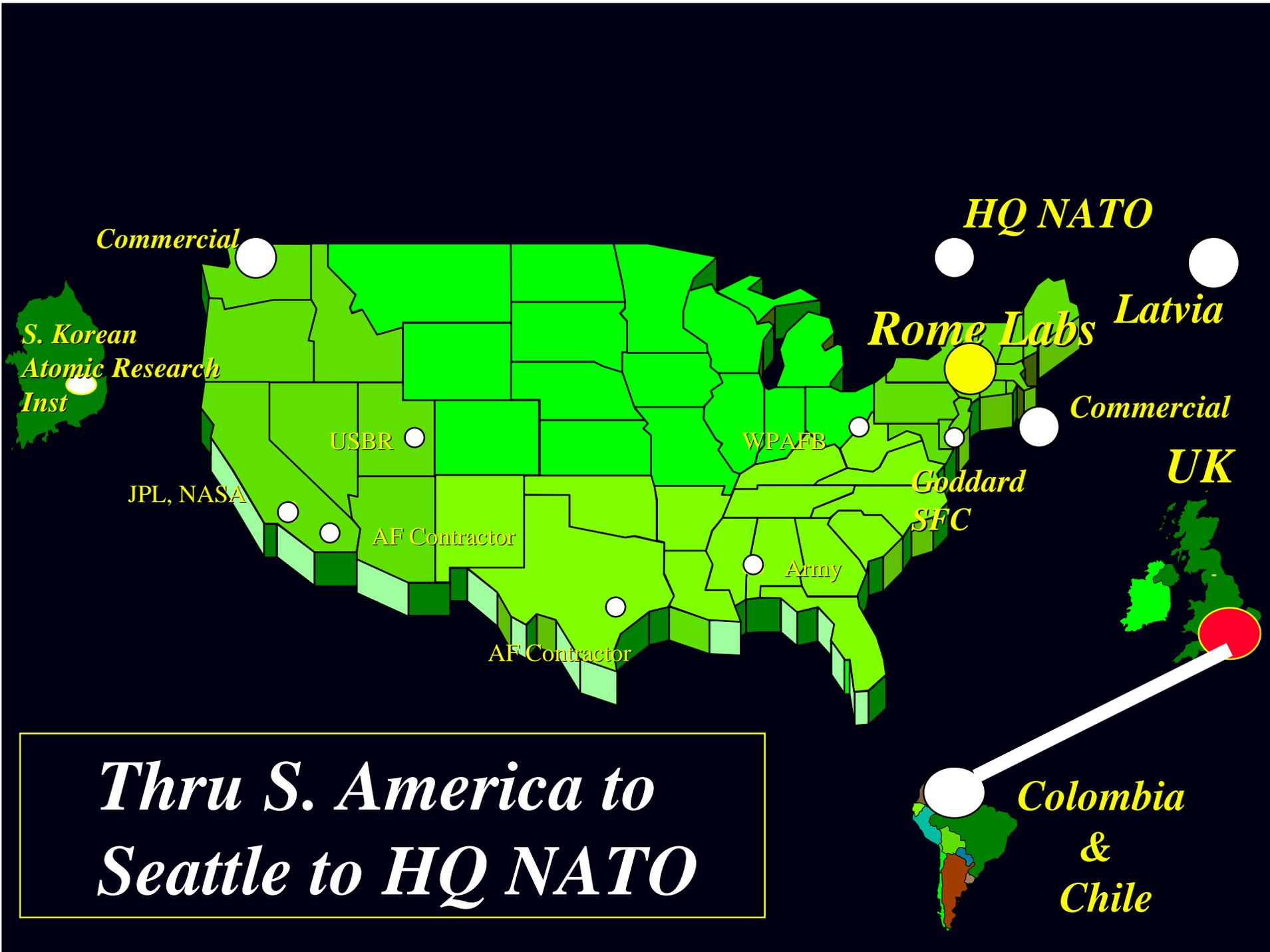
Followed Contracts

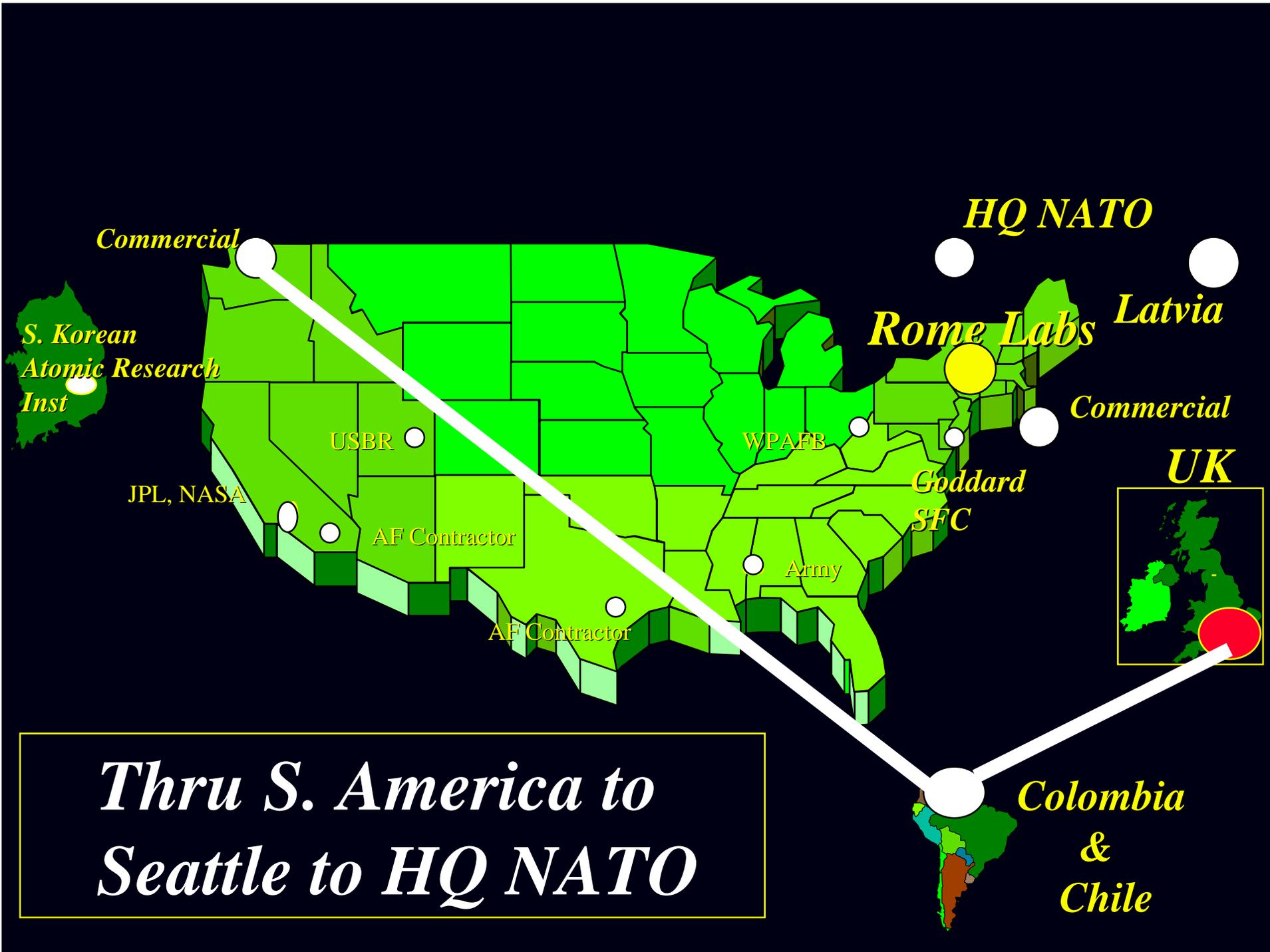


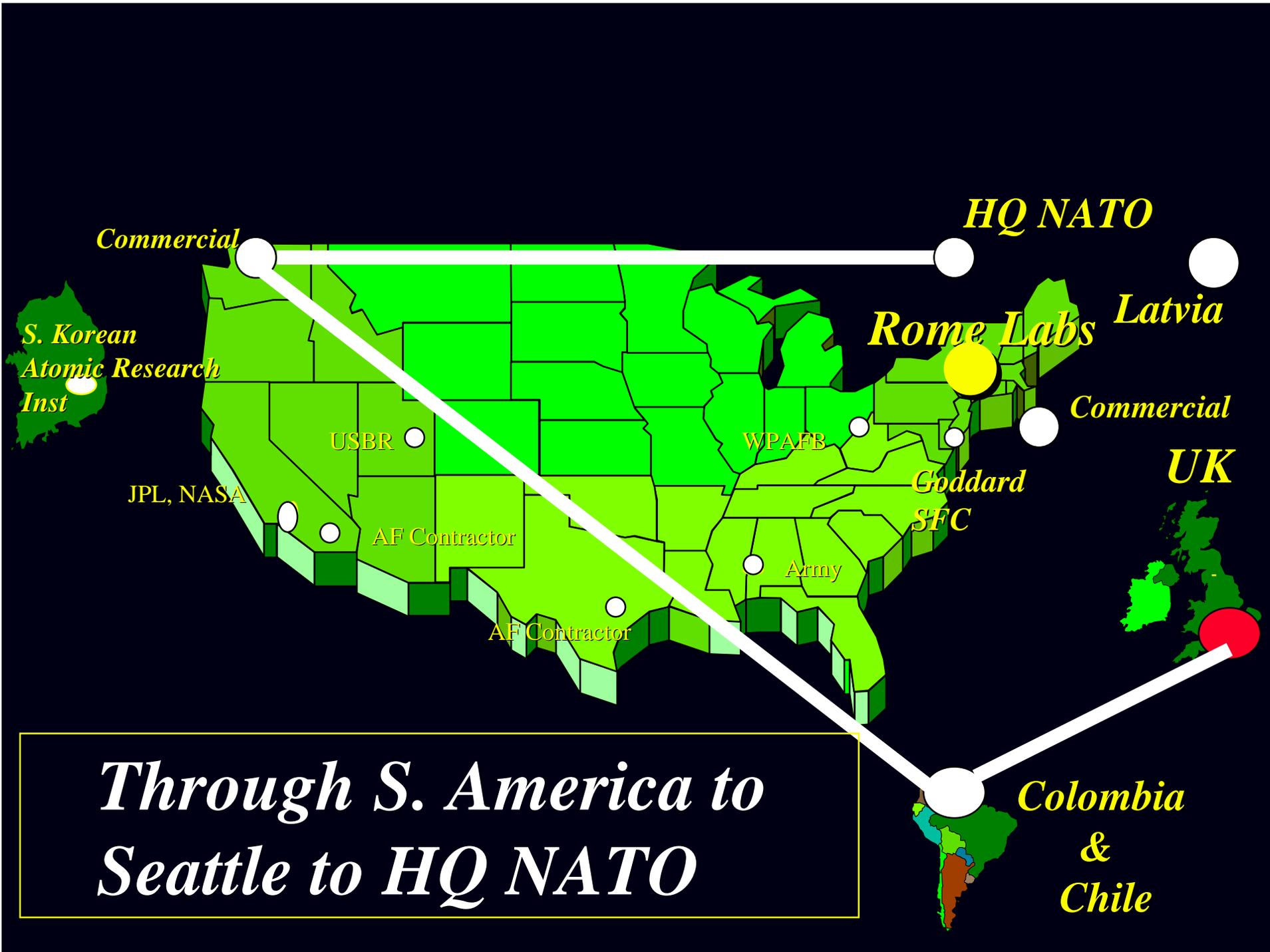
Followed Contracts

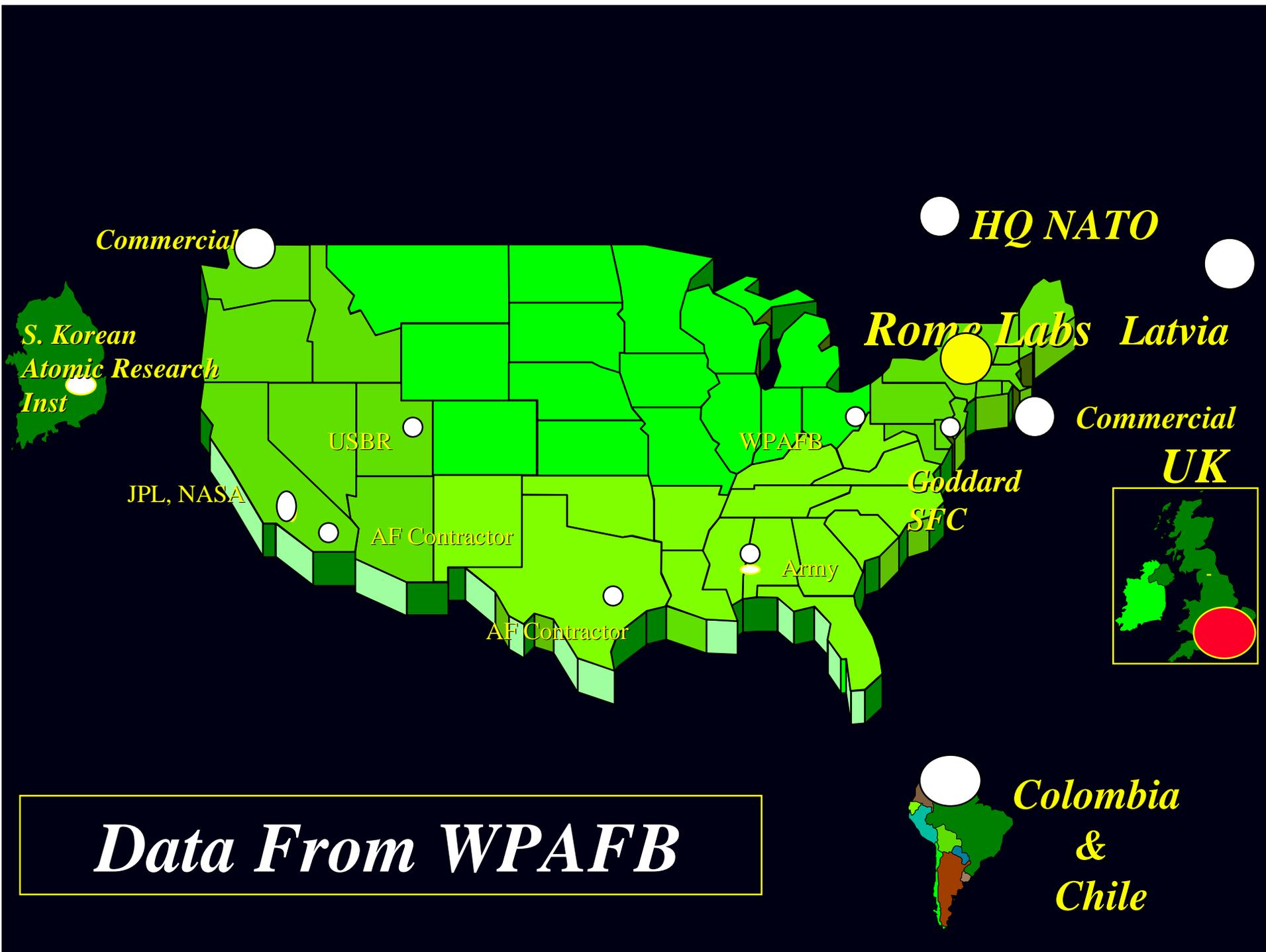












Commercial

*S. Korean
Atomic Research
Inst*

USBR

JPL, NASA

AF Contractor

AF Contractor

WPAFB

Army

*Goddard
SFC*

HQ NATO

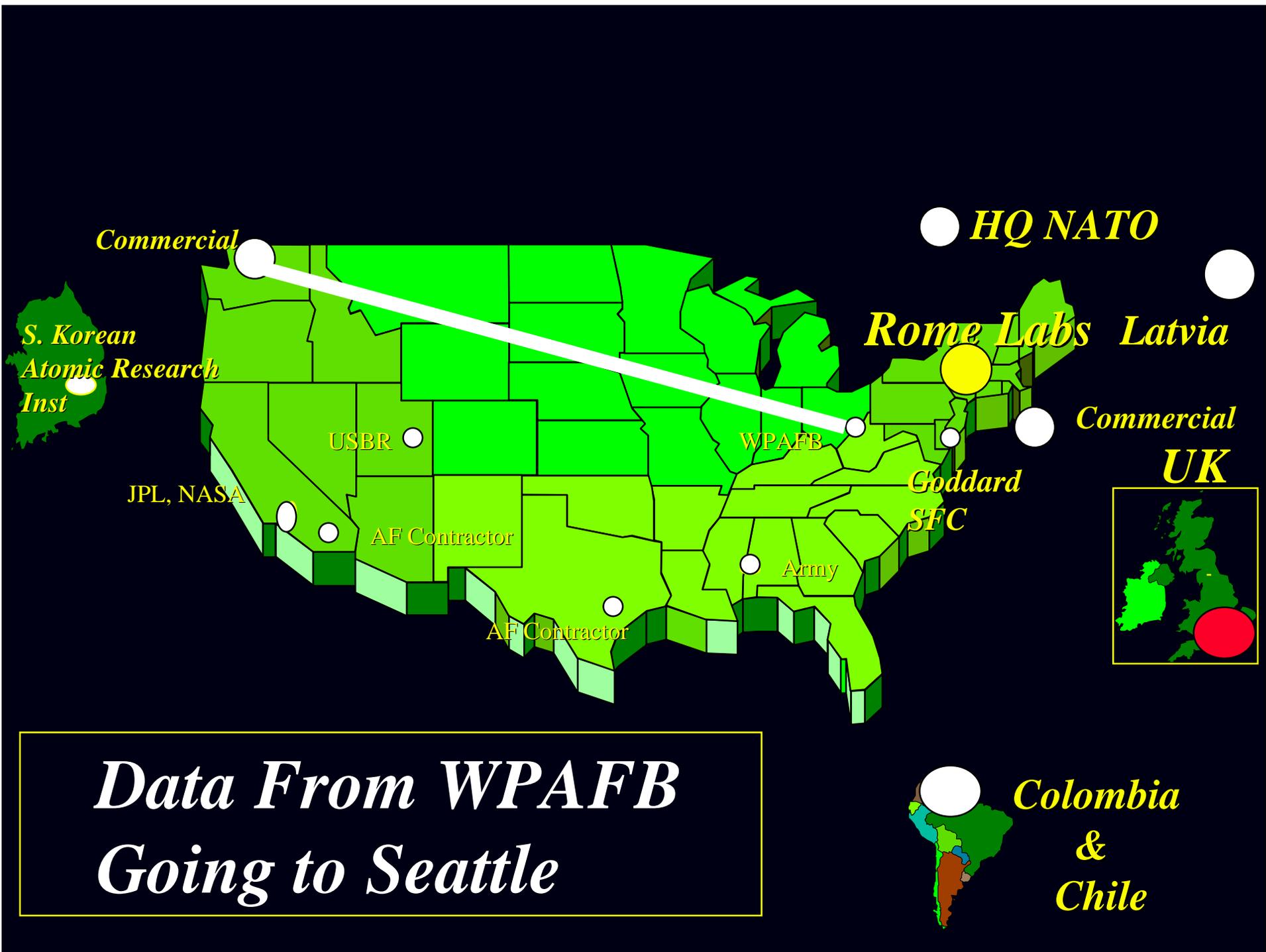
Rome Labs Latvia

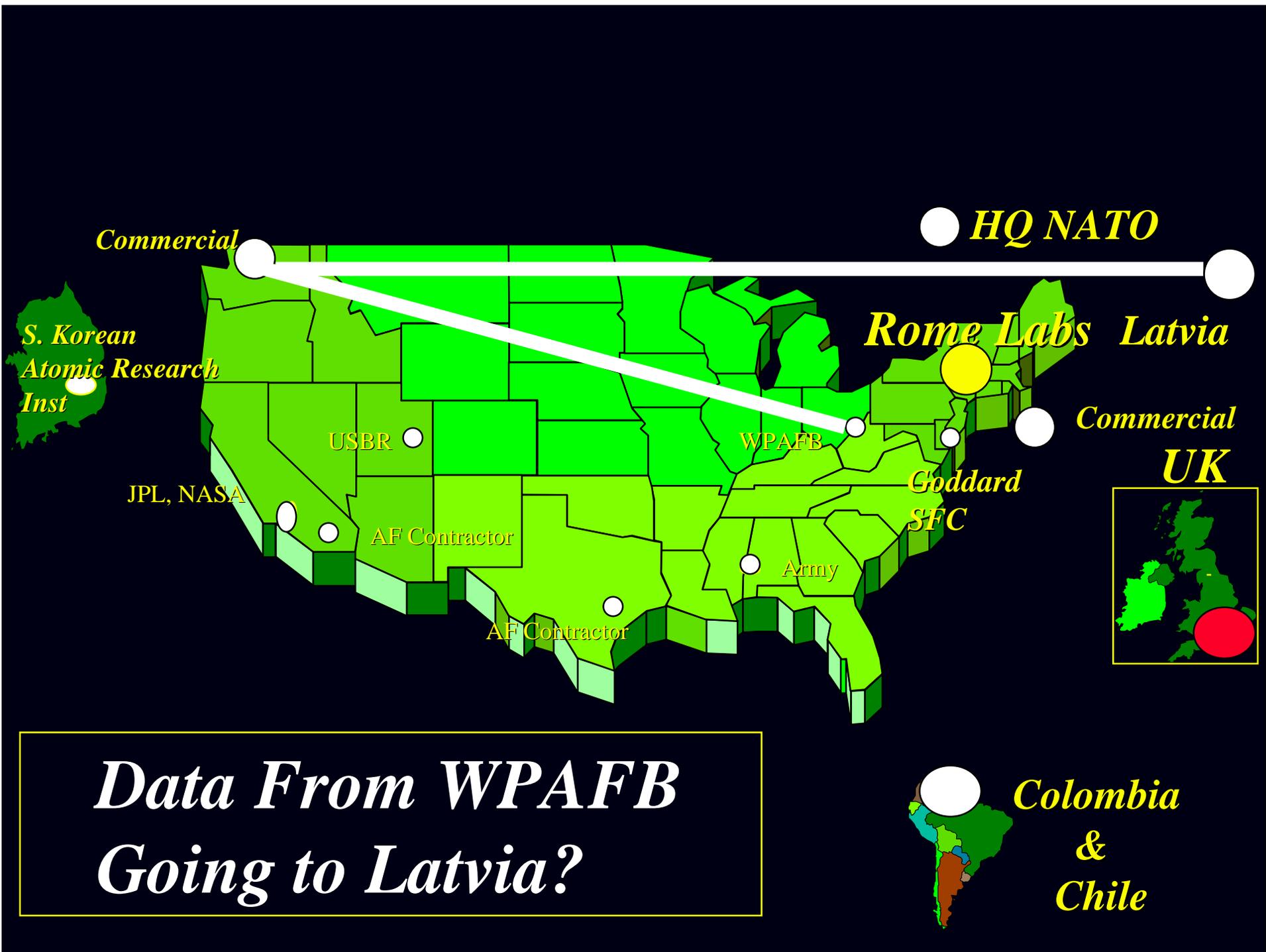
*Commercial
UK*



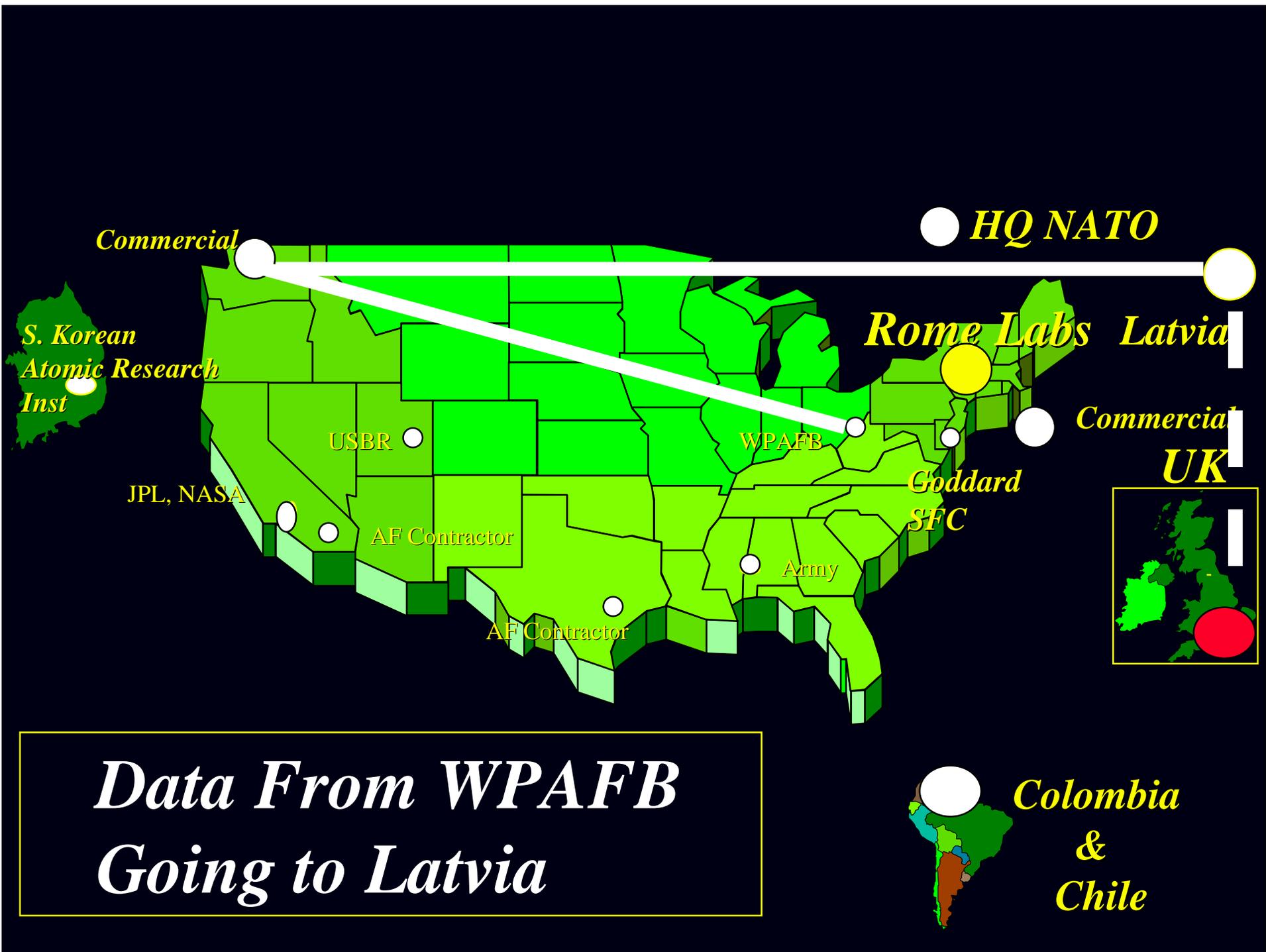
*Colombia
&
Chile*

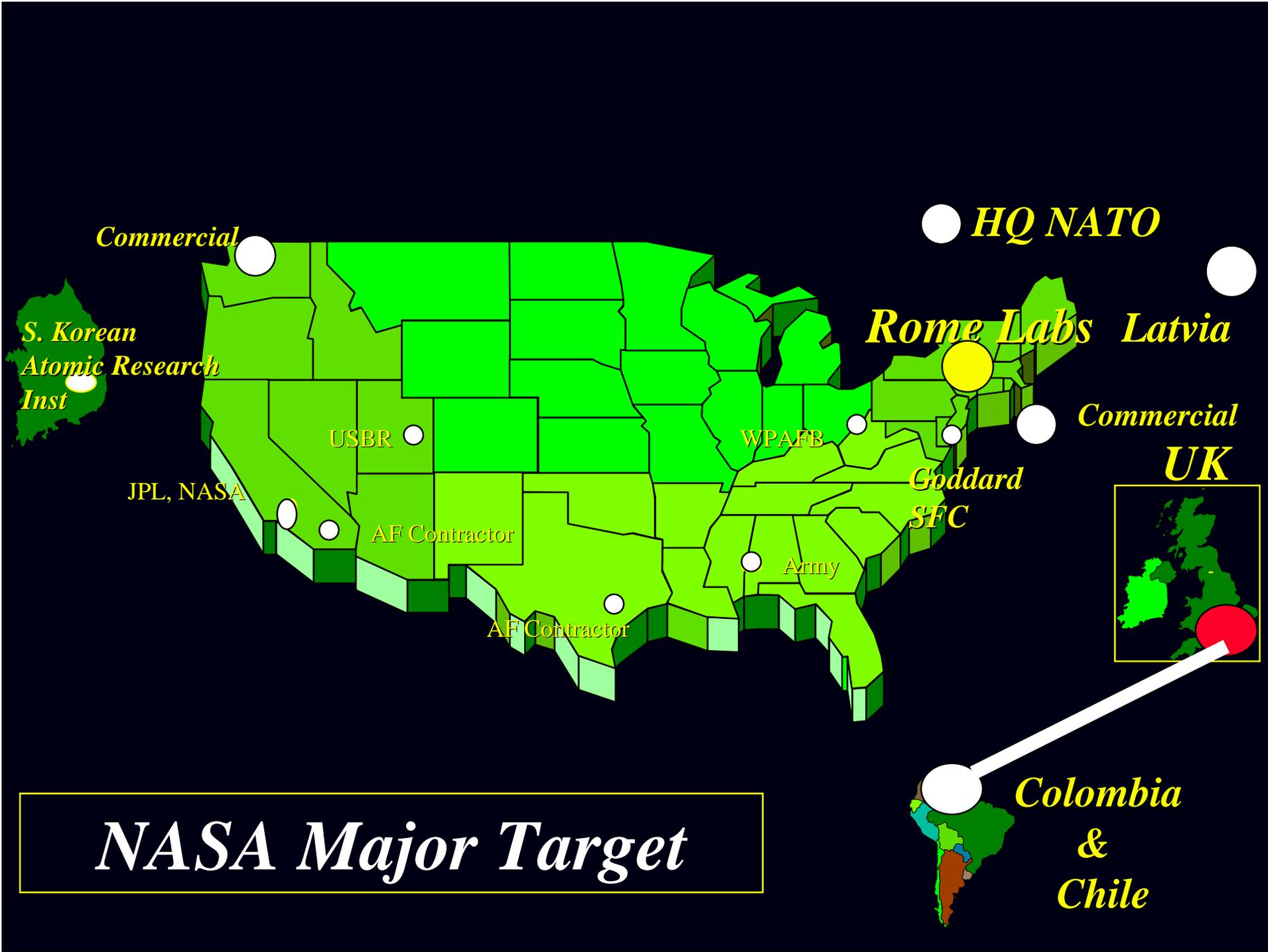
Data From WPAFB





*Data From WPAFB
Going to Latvia?*





Commercial

*S. Korean
Atomic Research
Inst*

USBR

JPL, NASA

AF Contractor

AF Contractor

WPAFB

Army

*Goddard
SFC*

HQ NATO

Rome Labs Latvia

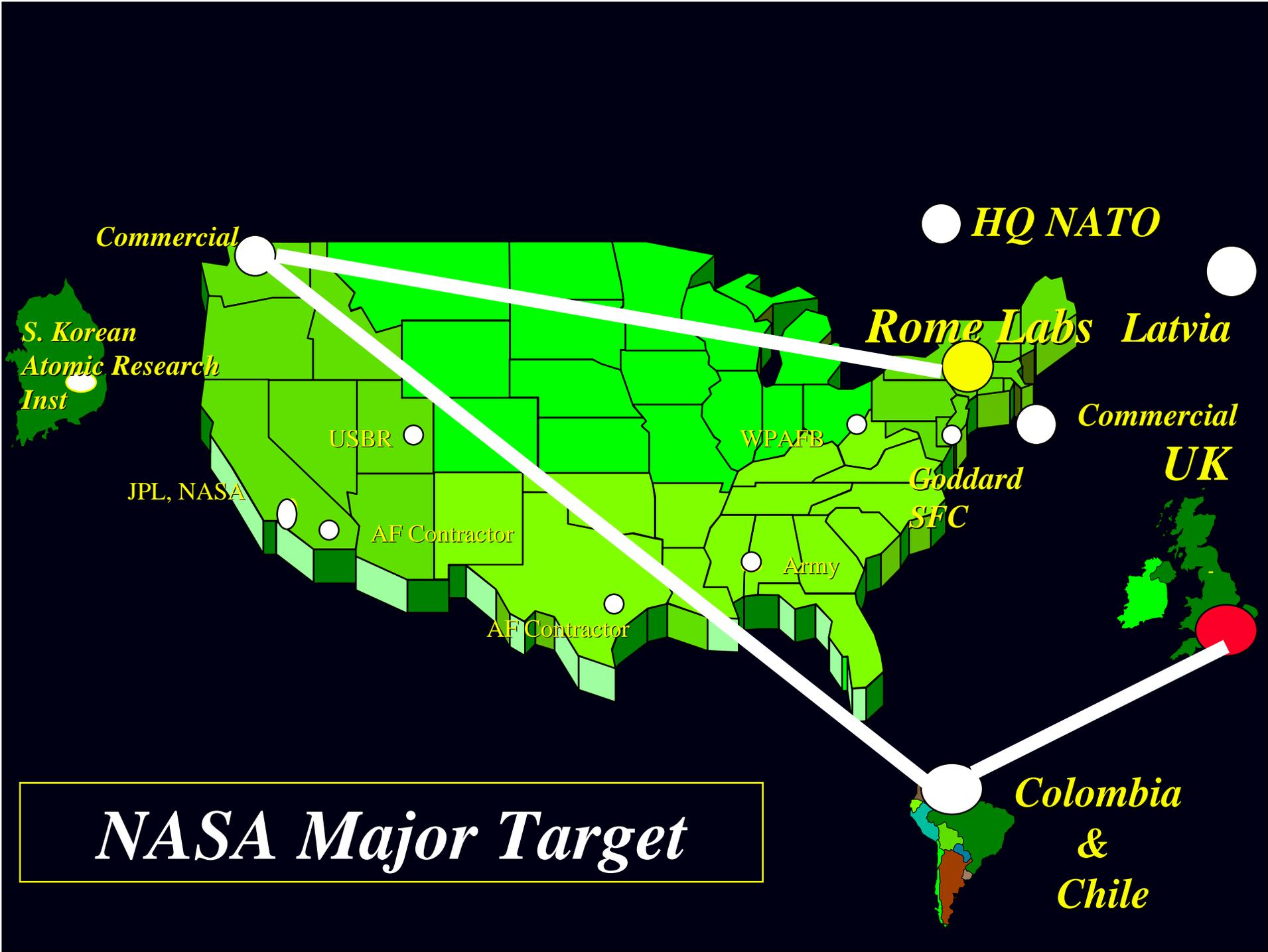
*Commercial
UK*

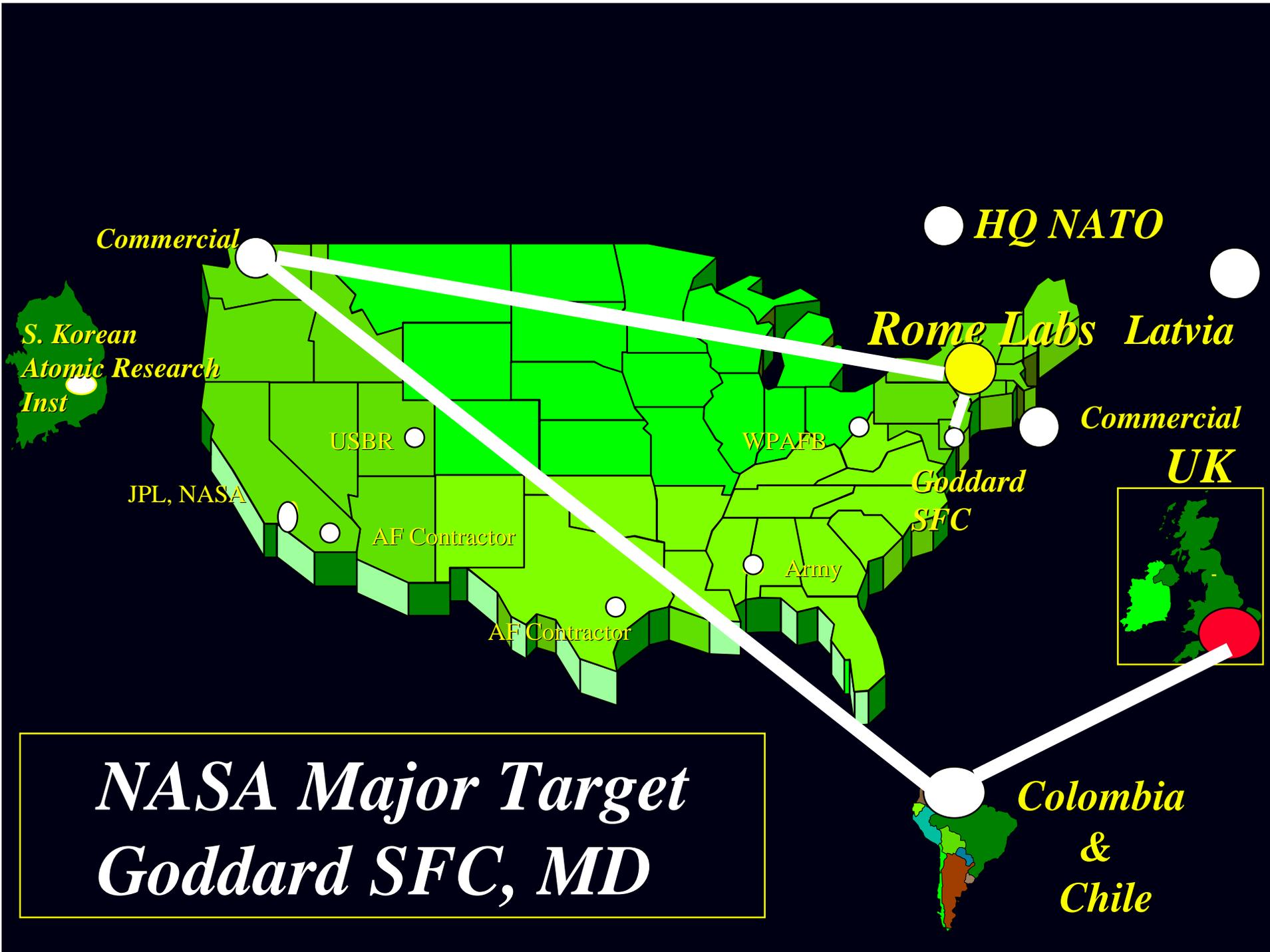


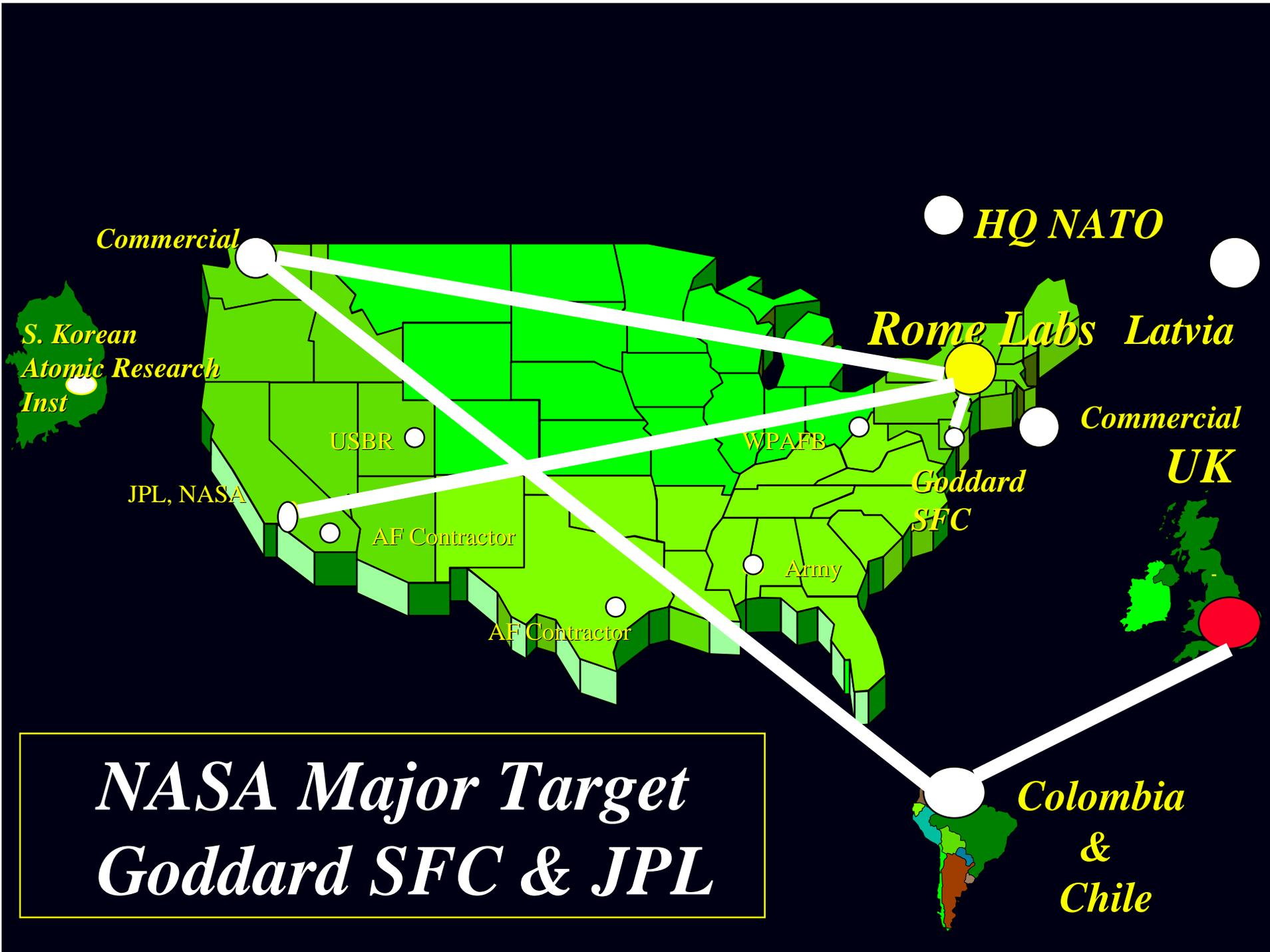
*Colombia
&
Chile*

NASA Major Target



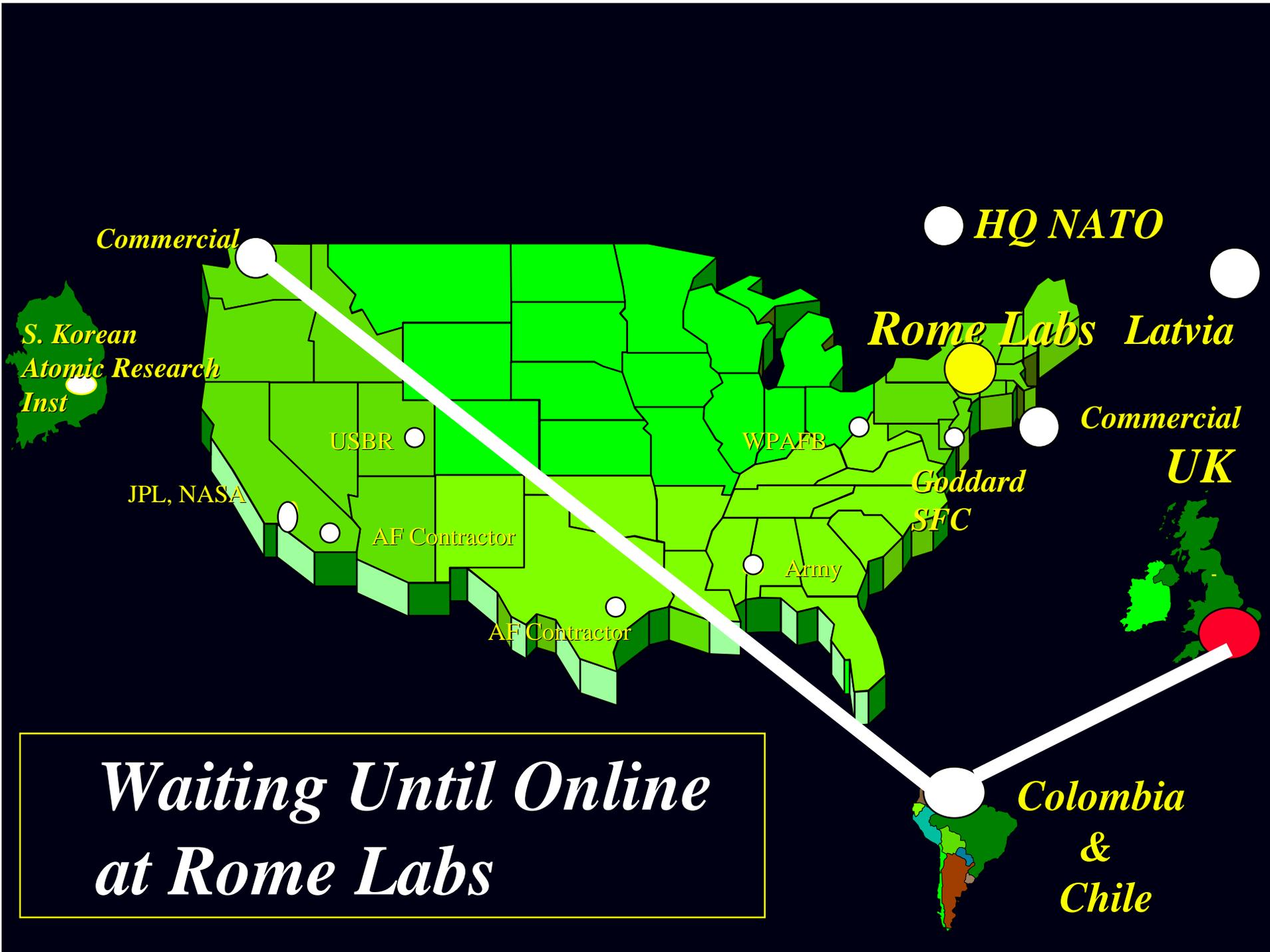


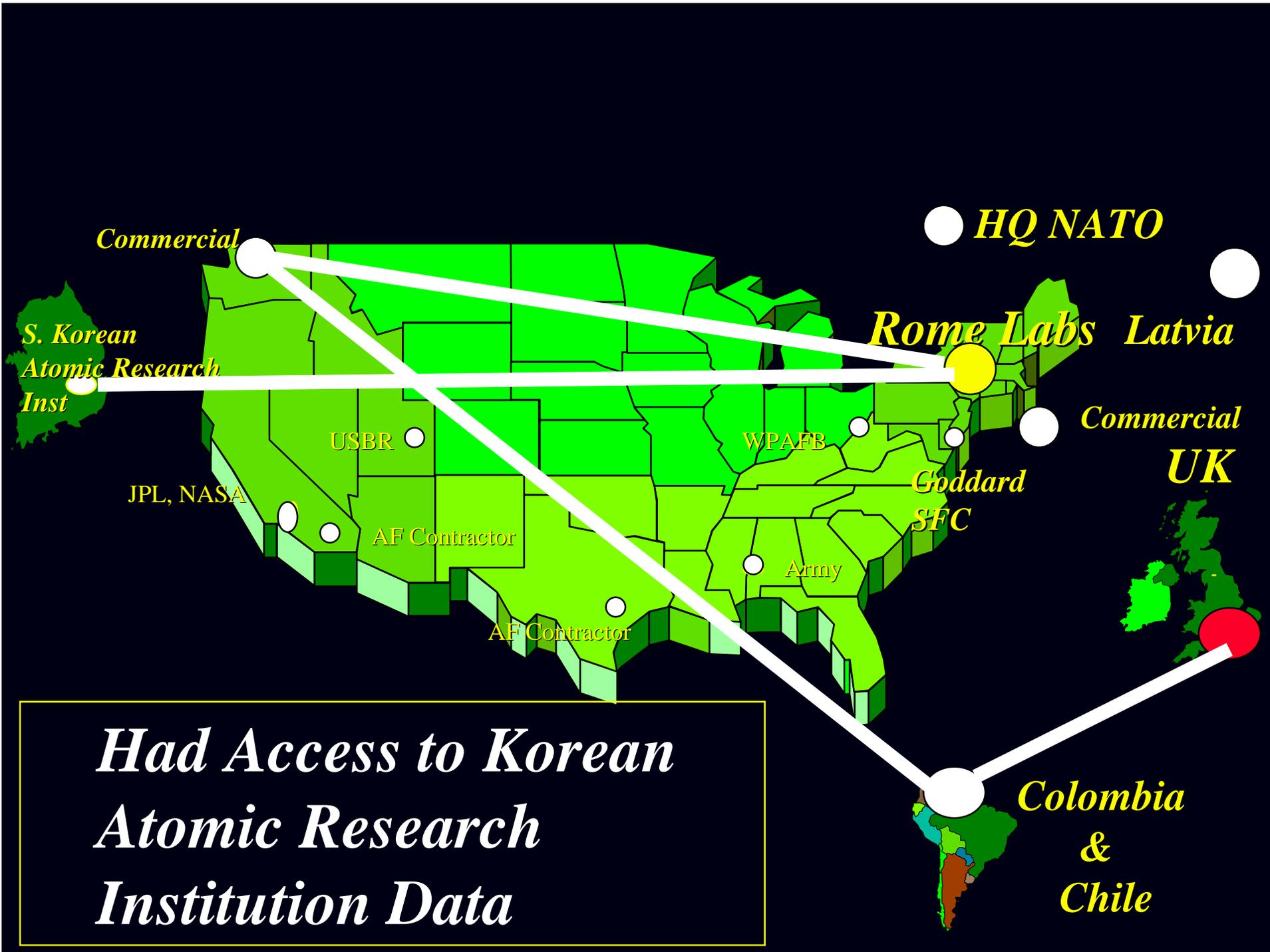


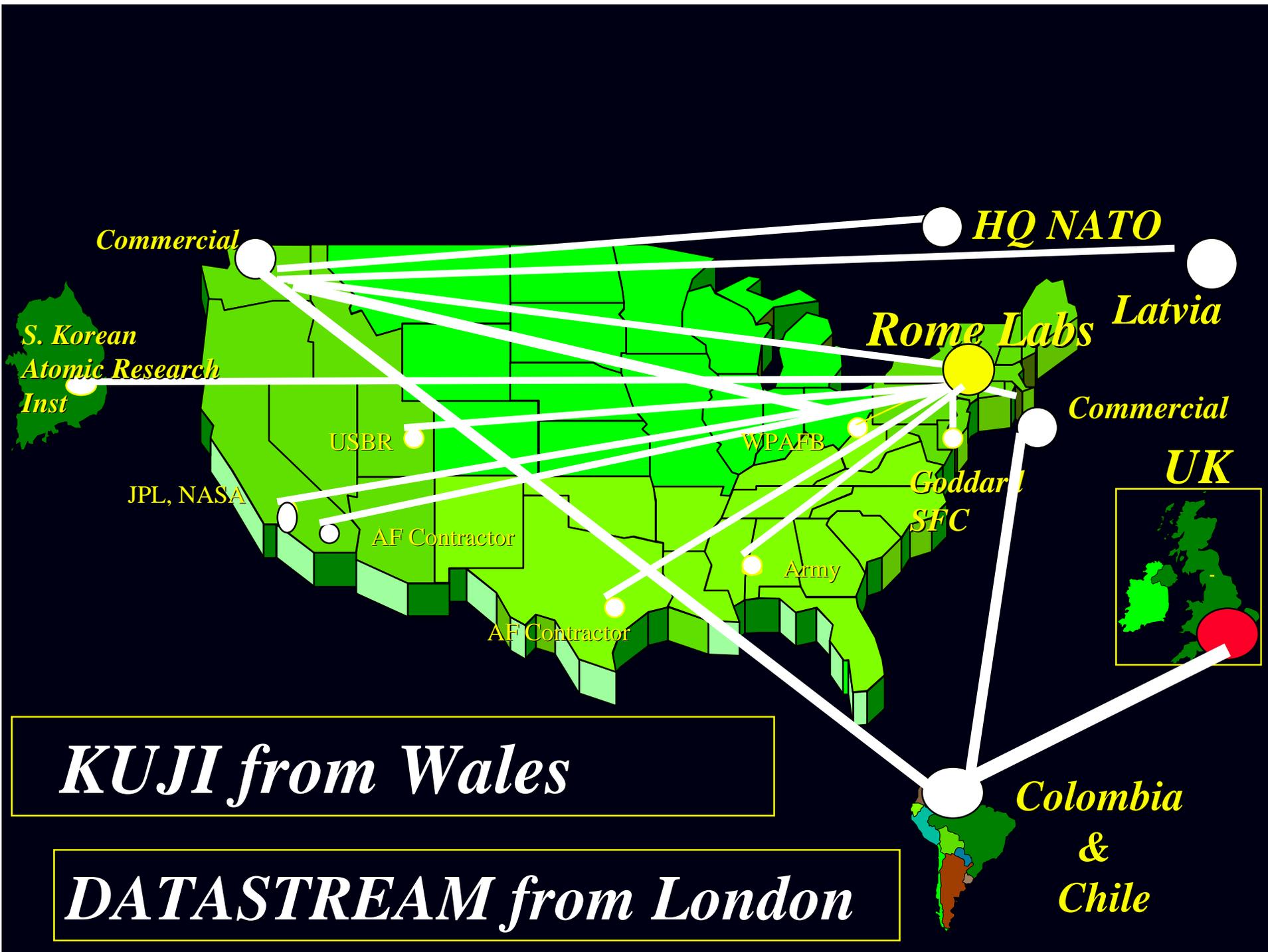


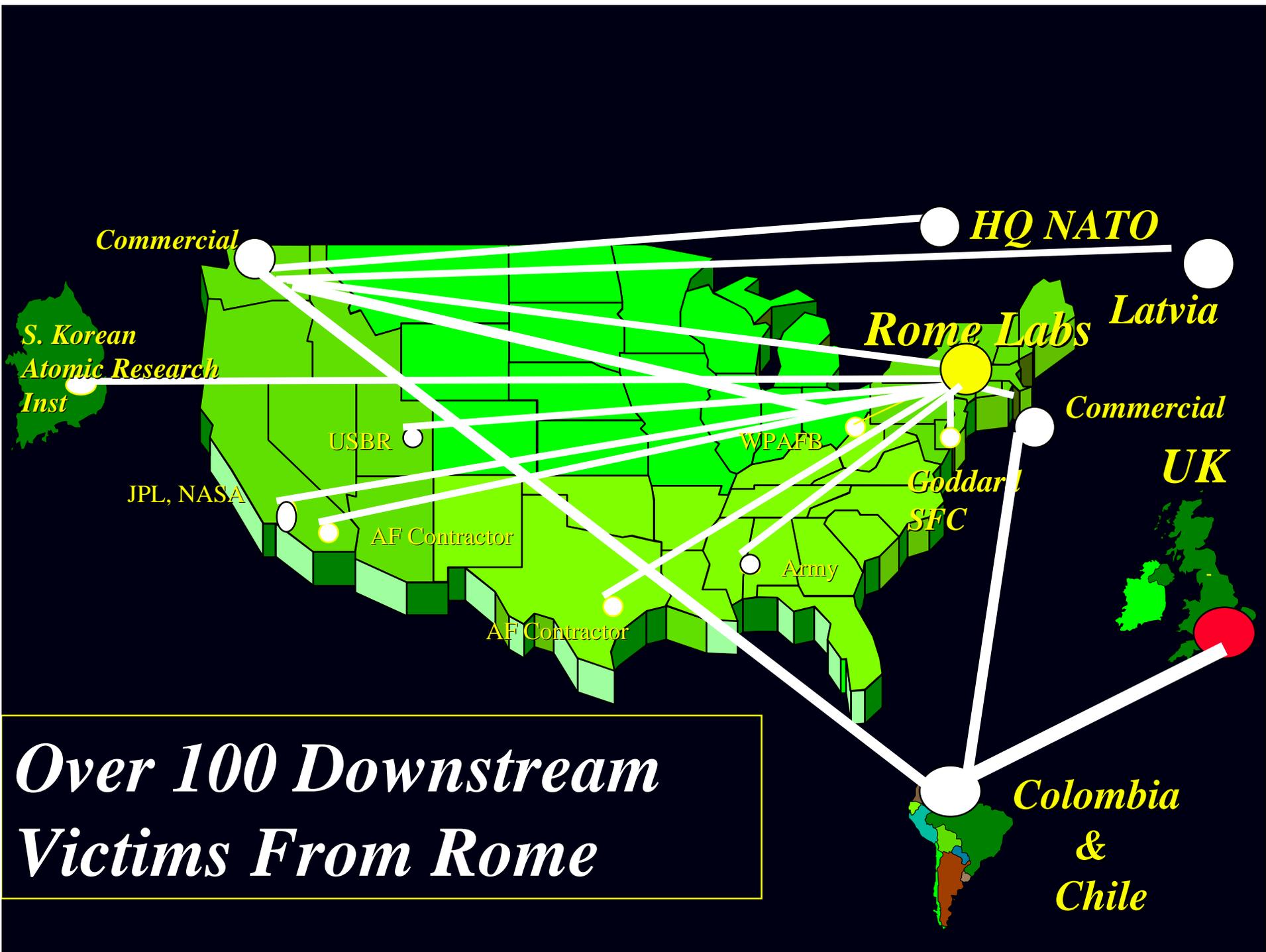


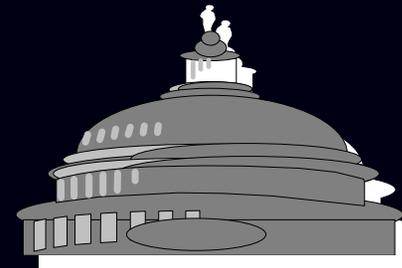








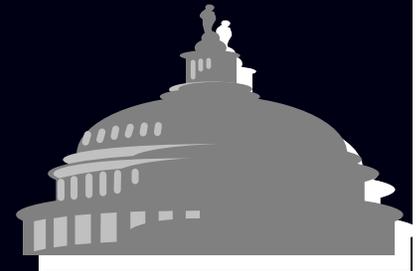




Rome Labs Summary

- *2 Hackers*
- *26 Days of Attacks*
- *20 Days of Monitoring*
- *7 Sniffers on Rome Systems*
- *Over 150 Intrusions at ROME Labs from 10
Different Points of Origin*
- *Victims - Many & Varied*
- *Law Enforcement Agencies - Multiple*
- *At Least 8 Countries Used as Conduit*





Bad Actors in the Physical World

Disaffected Loners

**Unabomber
Oklahoma City**

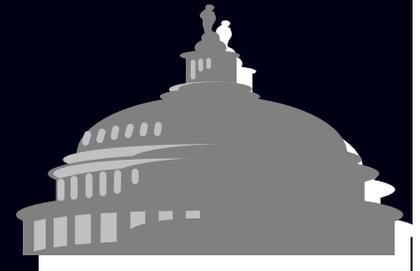
Subnational Threat

**Aum Shinrikyo
World Trade Center**

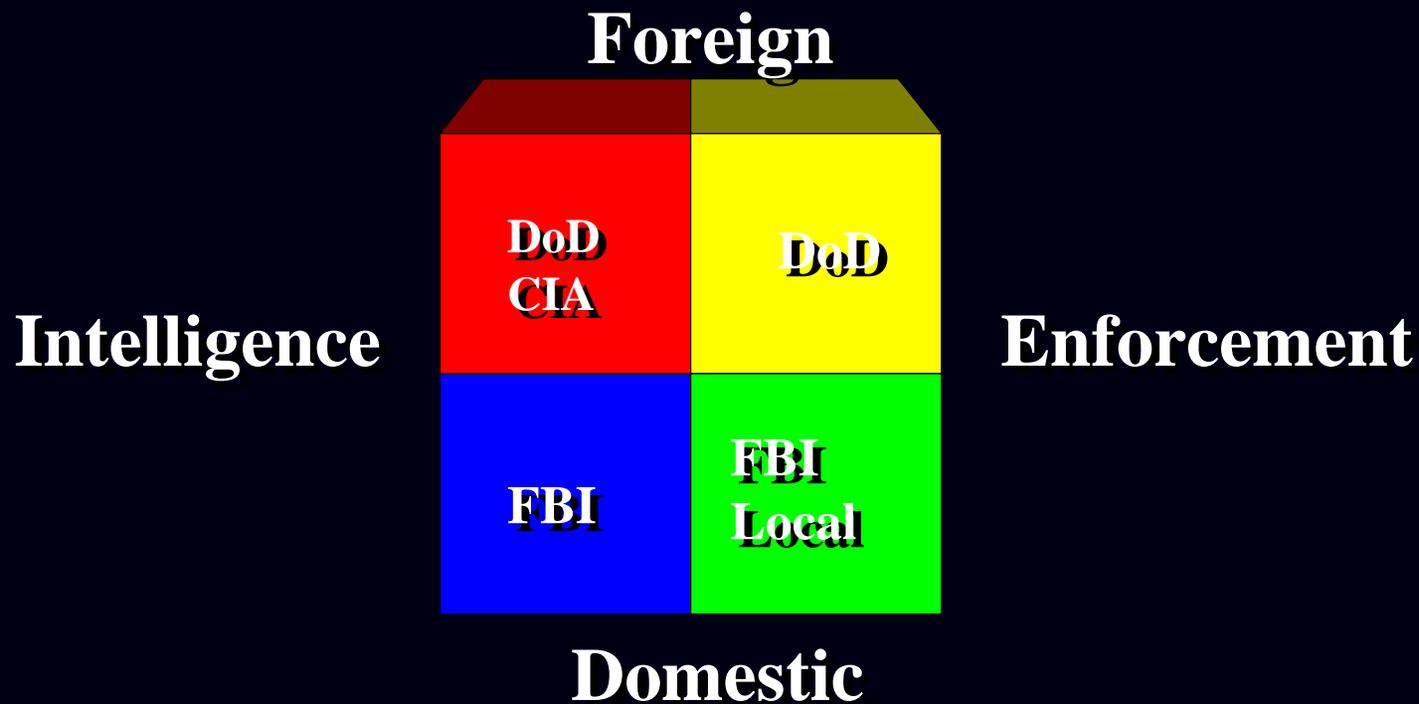
Rogue States

**Iraq
North Korea**

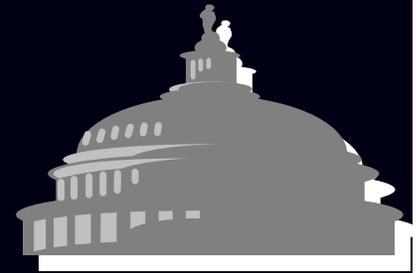
Defense-Wide Information Assurance Program



Promoting Our National Security In The Physical World



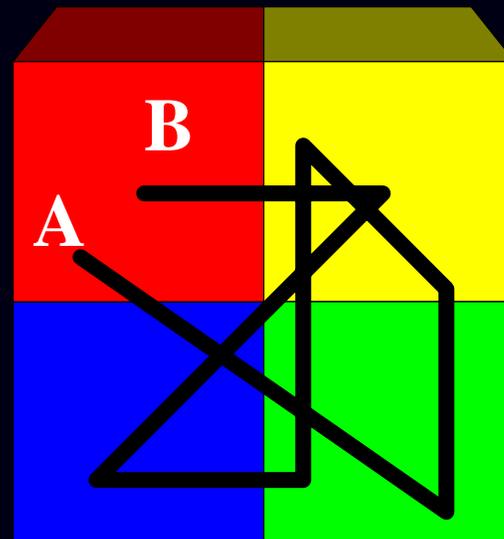
Defense-Wide Information Assurance Program



*Promoting Our National Security
In The Virtual World*

Foreign

Intelligence



Enforcement

Domestic

Defense-Wide Information Assurance Program

*National
Information Infrastructure*

Military/Gov Sys

Public Switch Nets

Transportation Sys

Financial Sys

Health Care Sys

Utilities/Power

Minimum Essential Pillars of Critical Elements



Proposed DoD Cyber Analysis Action Plan

*Special Agent Jim Christy, AFOSI
Special Assistant for Law Enforcement*

*Directorate of Information Assurance & Protection
Assistant Secretary of Defense*

Command, Control, Communications, and Intelligence (ASDC3I)

Defense-Wide Information Assurance Program



Background - Solar Sunrise

- *Intrusions into DoD Systems Feb 98*
 - *During Iraq Weapons Inspection Crisis*
 - *Intruders Exploited Known Vulnerabilities in Sun Solaris Operating Systems*
 - *Some Evidence Indicted Attacks Coming from Middle East*
 - *Raised Concern that Intrusions Could be Initial Stages of an Asymmetrical, Pre-Emptive Attack By Iraq*

Defense-Wide Information Assurance Program



Goal

“...What I have in mind is to have the ability by the end of the year to have a Department-wide awareness of a cyber attack within 4 hours of the first attack, irrespective of location or system...”

**Dr. Hamre, DEPSECDEF
15 Feb 98 Memo**

Note: During Solar Sunrise

Defense-Wide Information Assurance Program



Goal

What That Means is:

Situational Awareness

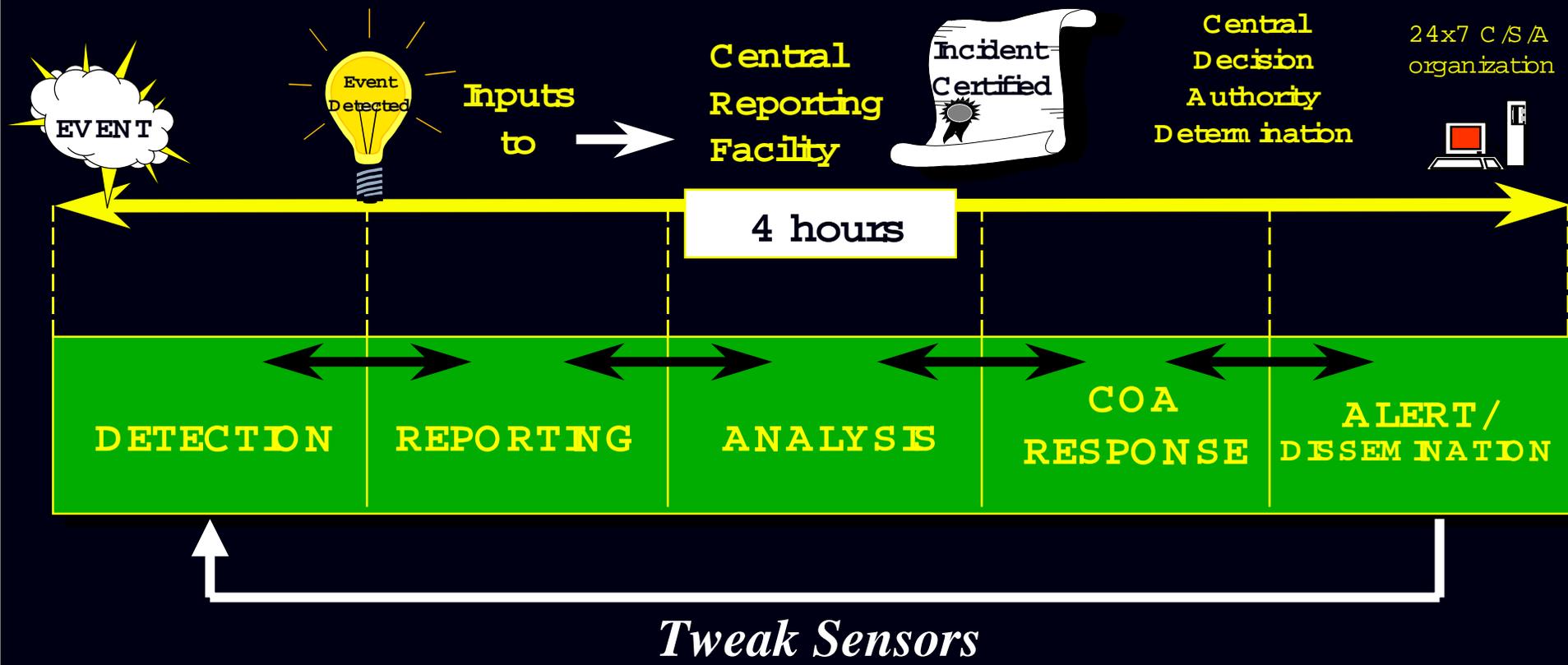
and a

Common Operating Picture

Defense-Wide Information Assurance Program



Critical Process



Defense-Wide Information Assurance Program



Current Posture

Today, we DO NOT meet the 4 hour GOAL

- Insufficient IDS*
- Insufficient Analytical Capability*
- Insufficient Notification System*
- Insufficient Training, Personnel, and Incentive Programs*
- No Formal Reporting/Alert/Notification/Training Process*

Can't Get There From Here!

Defense-Wide Information Assurance Program



Process Must Tie Together Into a System

- *Intrusion Detection Sensors*
- *Data from Sensors*
- *CERTs*
- *NOCs*
- *INFOCONs*
- *IAVA System*
- *Law Enforcement Evidence*
- *Intelligence Community
Collections/Analysis*
- *Non-DoD Related Incidents*

*Situational
Awareness*

Defense-Wide Information Assurance Program



Defense In Depth

People

Training

Certification

Awareness

Systems Security

Physical Security

Personnel Security

Cyber Cops

Technology

Defense in Layers

Security Criteria

IT/IA Acquisition

Risk Assessments

C&A

PKI

Forensic Tools

Operations

Assessment

Monitoring &

Analysis

Warning

Response

Reconstitution

LE Investigations

CI Operations

Defense-Wide Information Assurance Program

Incident Attack

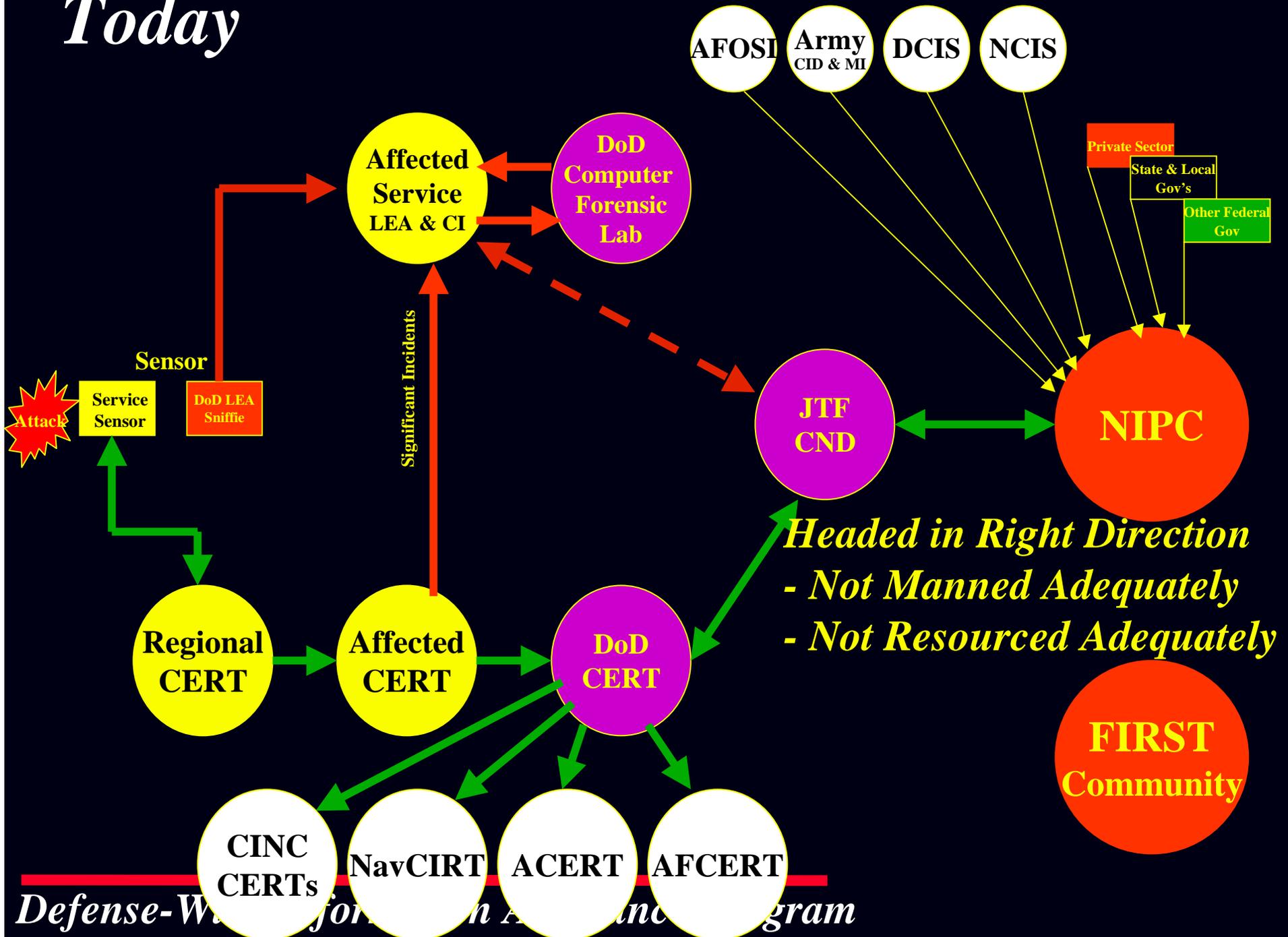
Event

Attackers	Tool	Vulnerability	Action	Target	Unauthorized Result	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge, Status, Thrills
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

Taxonomy



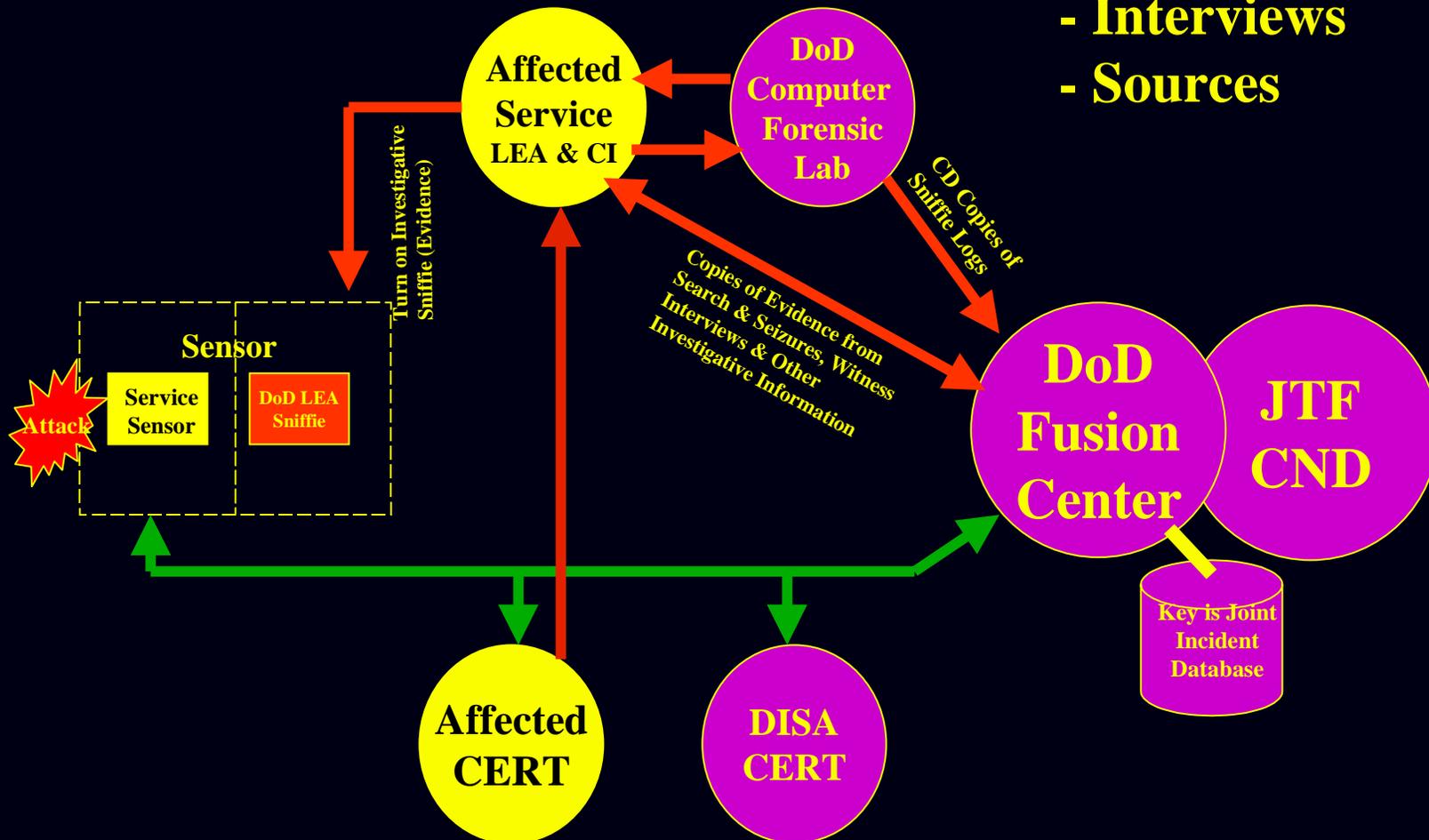
Today



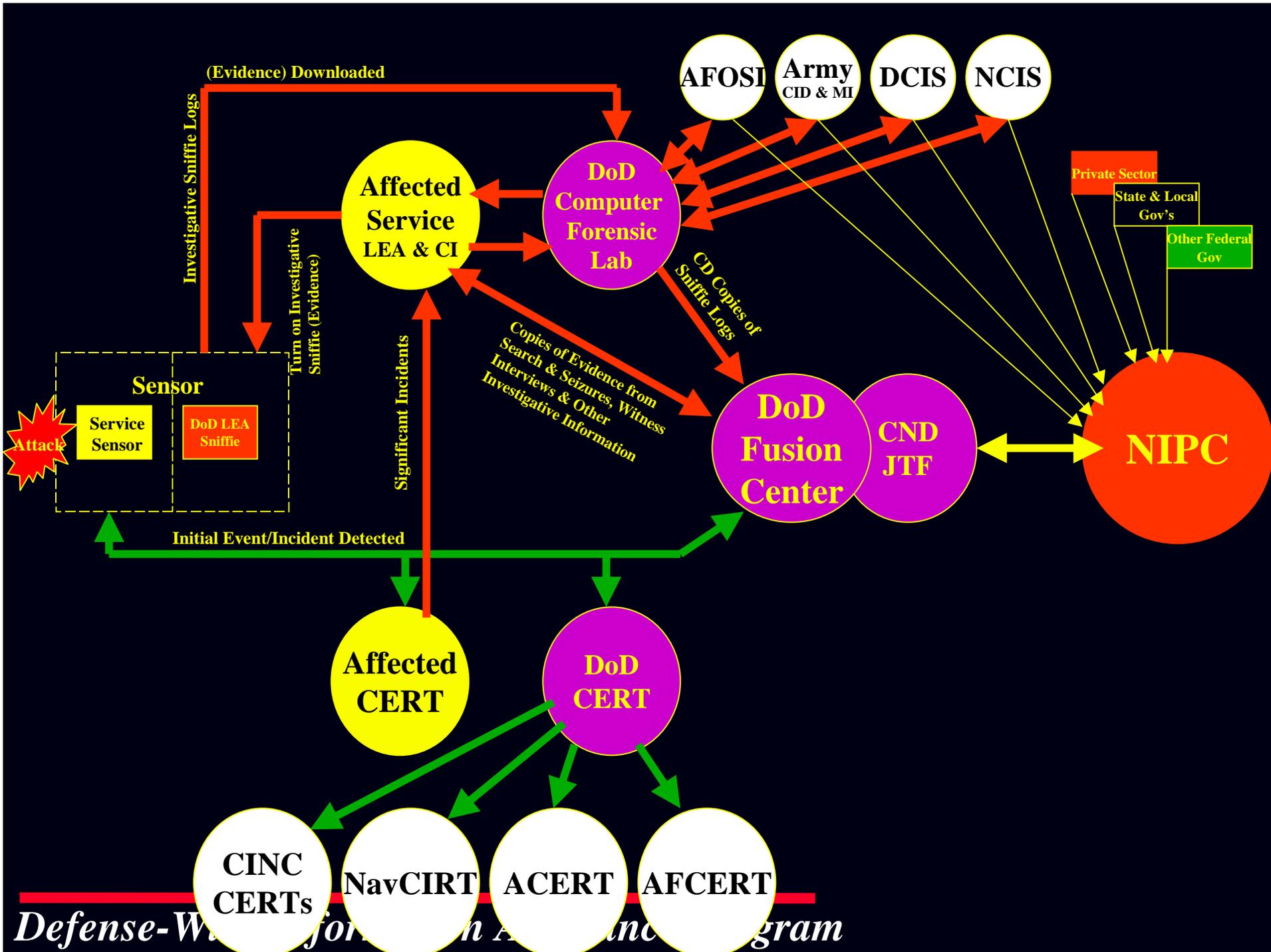
Proposed Future

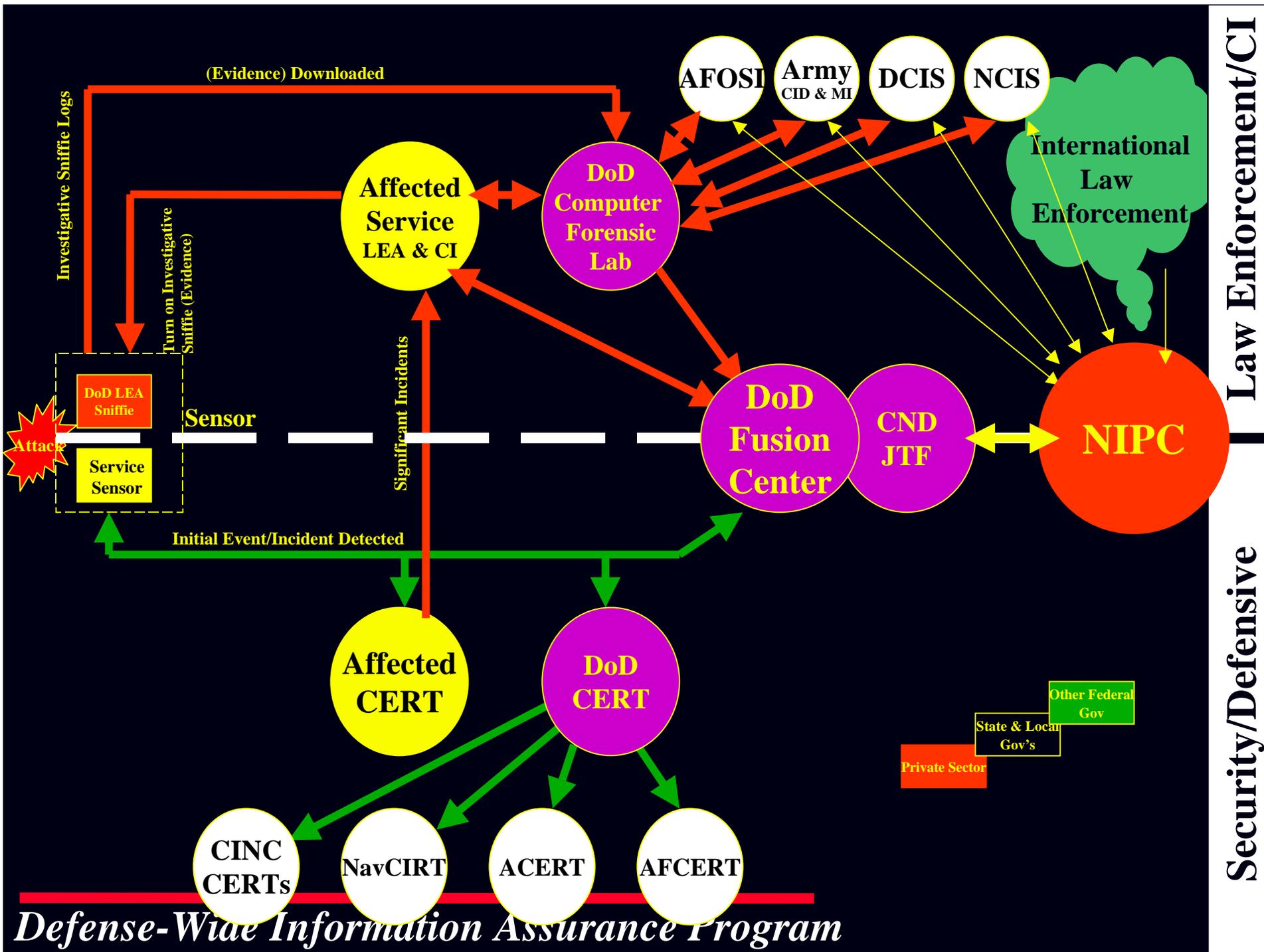
Valuable LE Info From

- Search Warrants
- Court Orders
- Interviews
- Sources



Defense-Wide Information Assurance Program

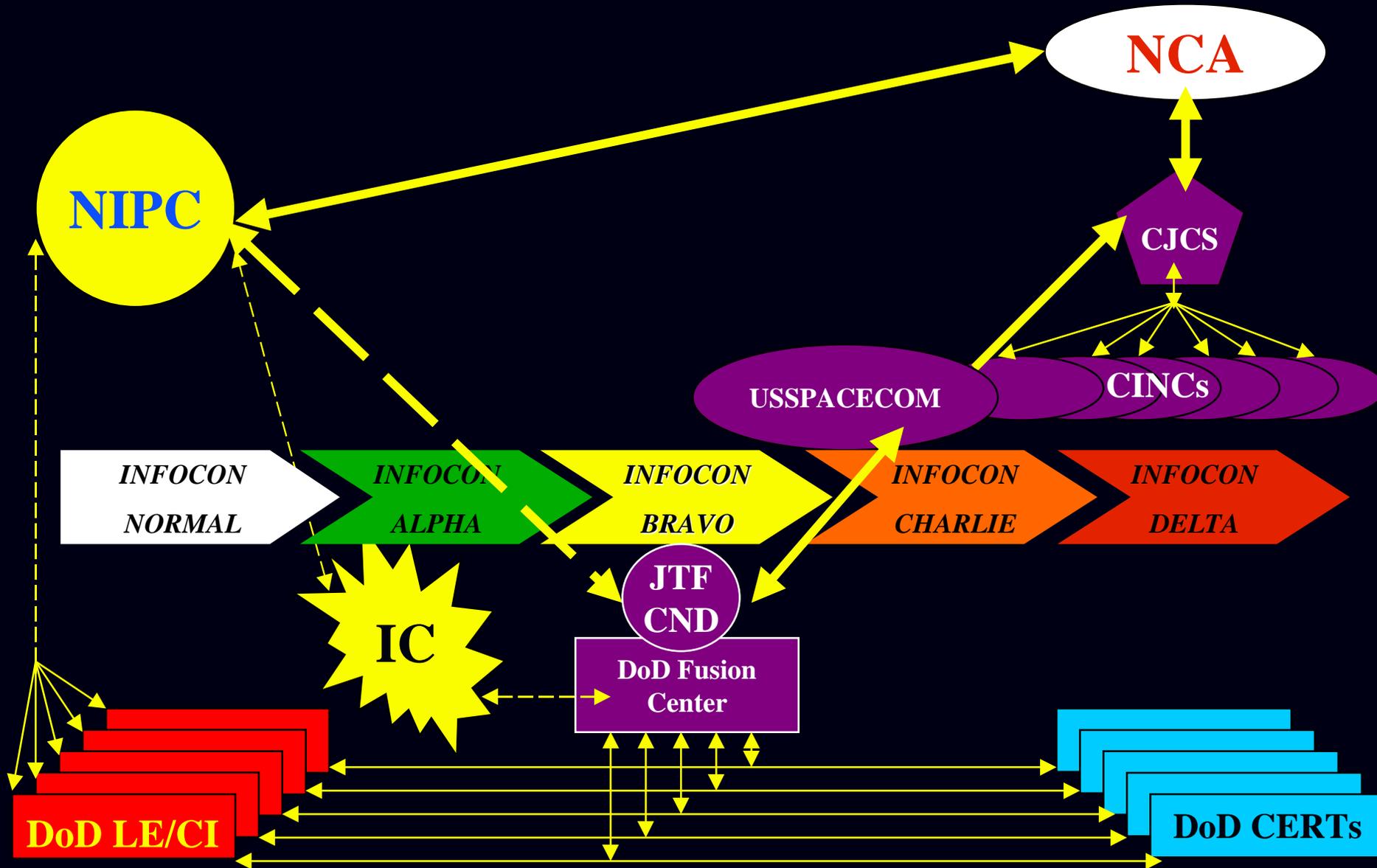




PEACE

CRISIS

WAR

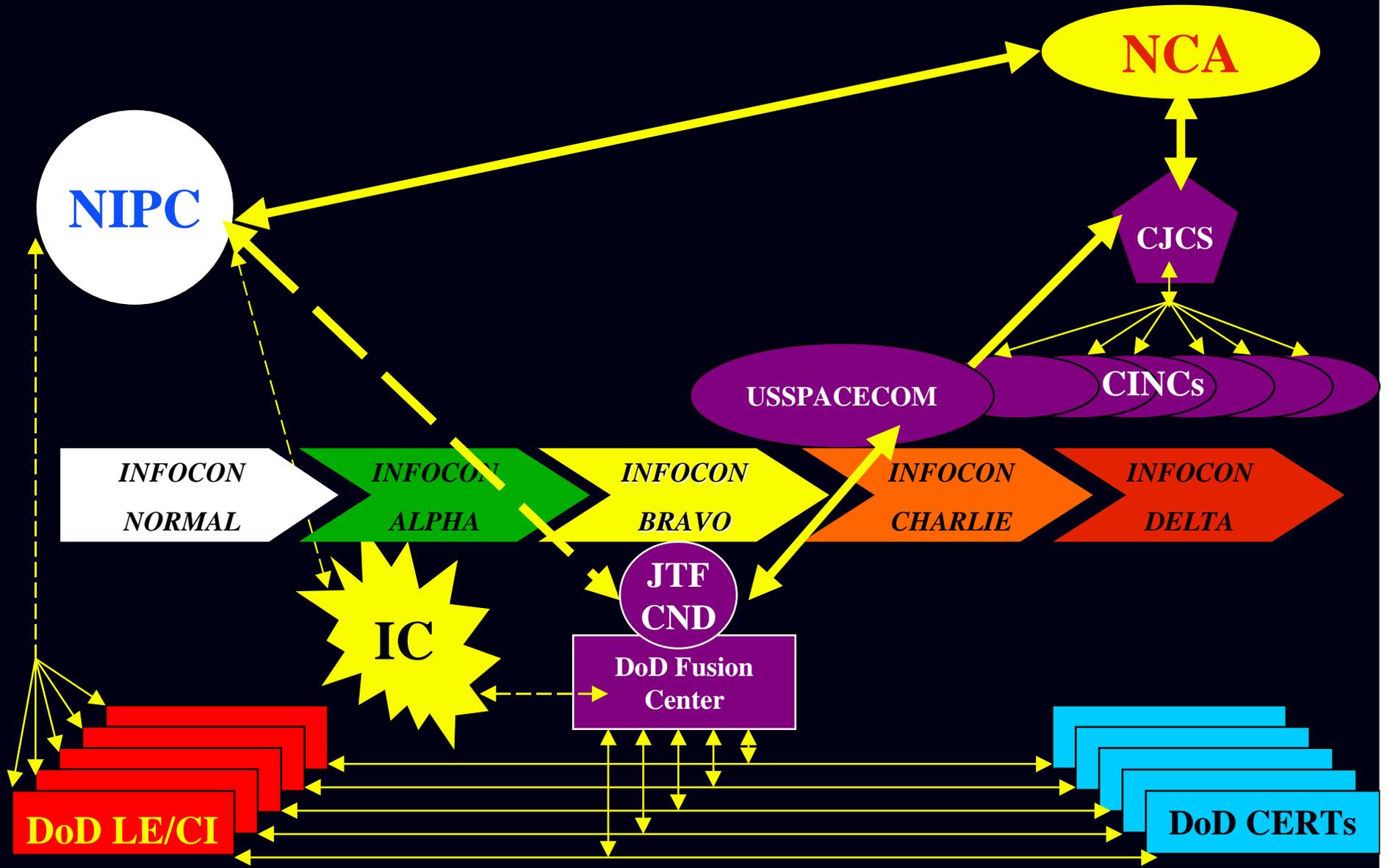


Defense-Wide Information Assurance Program

PEACE

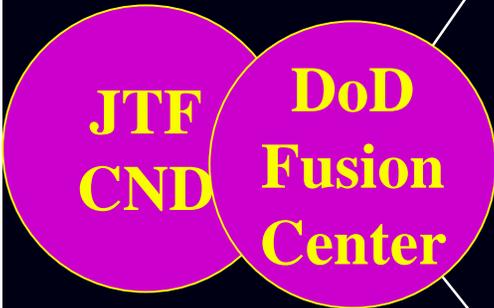
CRISIS

WAR



Defense-Wide Information Assurance Program

Fusion of Information & Disciplines



Law Enforcement & CI

AFOSI - Criminal & CI
NCIS - Criminal & CI
DCIS - Criminal
Army CID - Criminal
Army MI - CI
DoD Computer Forensic Lab

Intelligence

NSA - SIGINT & InfoSec
X Group
NSIRC
DIA - All INTs

CERTs

AFCERT
NavCIRT
ACERT
DOD CERT
CINC CERTs

Operators

J39
J6K
J2
CND Joint Task Force
NCS
DISA GNOSC

Who? Where? Why?

What?, When? How?

Defense-Wide Information Assurance Program



Bottom Line

*To Protect Our Systems It Will Require
Input From:*

- CERTs & SysAdms*
- Law Enforcement*
- Counterintelligence*
- Intelligence*
- DoD Infrastructure*
- Private Sector*
- Other OGAs*

A Fusion of Disciplines is Required!

Defense-Wide Information Assurance Program



DOD Computer Network Defense Centers and Activities Study

Defense-Wide Information Assurance Program

Project Overview



The overall objective of the study is to

Phase 1

- *Document the charter, manpower, and resources of the centers*
- *Identify those external centers with which DOD centers interface*
- *Map the interrelationships between the centers, programs and activities*

Phase 2

- *Examine the interfaces that DOD centers have with external centers and identify impacts of the external centers on DOD resource requirements*

Phase 3

- *Identify gaps in capability and potential redundancies; assess opportunities for synergy, improved mission effectiveness, and manpower efficiencies*
- *Provide alternative organizational constructs to optimize DOD's DIO force structure and operations*

Defense-Wide Information Assurance Program



Data Collected on the Following Centers

- **Joint Task Force -Computer Network Defense**
- **Global Operations and Security Center**
- **Air Intelligence Agency**
- **Joint Command and Control Warfare Center**
- **Naval Information Warfare Activity**
- **Fleet Information Warfare Center**
- **Land Information Warfare Activity**
- **Defense Criminal Investigation Service**
- **Air Force Office of Special Investigations**
- **Naval Criminal Investigation Service**
- **Army Criminal Investigation Directorate**
- **Army Military Intelligence**
- **DIA Transnational Warfare Group**
- **X Group - NSA**
- **Information Operations Technology**
- **DOD Computer Forensic Laboratory**
- **Joint Spectrum Center**
- **Joint Warfare Analysis Center**
- **Joint C4I Battle Center**

Defense-Wide Information Assurance Program



Centers Visited

- **US Space Command**
- **Joint Chiefs of Staff, J-2 Military Intelligence**
- **Army Network Operations Center**
- **Naval Computer and Telecommunications Command**
- **Unified Atlantic Network Operations Center**
- **Air force Network Operations Center**
- **USMC Network Operations Center**
- **Army Research Laboratory**
- **Defense Logistics Agency**
- **Defense Advanced Research Projects Agency**
- **National Infrastructure Protection Center**
- **CIA Office of Transnational Issues**

Defense-Wide Information Assurance Program



CND Organizations and Activities Study

35 Organizations Assessed

Protection	CERTs	Network Operations	Support
<ul style="list-style-type: none"> • Joint Task Force - Computer Network Defense • US Space Command • National Infrastructure Protection Center 	<ul style="list-style-type: none"> • Air Force Computer Emergency Response Team • Army Computer Emergency Response Team • Navy Computer Incident Response Team • Defense Logistics Agency CERT • National Security Agency (X Group) • Carnegie Mellon University CERT/CC 	<ul style="list-style-type: none"> • Air Force Network Operations Center • Army Network Systems Operations Center • Naval Computer and Telecommunications Command • Global Network Operations Security Center 	<ul style="list-style-type: none"> • Joint Command and Control Warfare Center • Joint Spectrum Center • DoD Computer Forensics Laboratory • Defense Advanced Research Projects Agency • Joint C4ISR Battle Center • Army Research Lab
IW	LE/CI	Intelligence	Other
<ul style="list-style-type: none"> • Air Force Information Warfare Center • Land Information Warfare Activity • Naval Information Warfare Activity • Fleet Information Warfare Center • Information Operations Technology Center 	<ul style="list-style-type: none"> • Air Force Office of Special Investigations • US Army Criminal Investigation Directorate • US Army Military Intelligence • Naval Criminal Investigation Service • Defense Criminal Investigative Service 	<ul style="list-style-type: none"> • Joint Staff - J2 • Defense Intelligence Agency • Air Intelligence Agency 	<ul style="list-style-type: none"> • National Aeronautics and Space Administration • Joint Warfare Analysis Center

Defense-Wide Information Assurance Program

Preliminary Mapping of CERT Support to JTF-CND

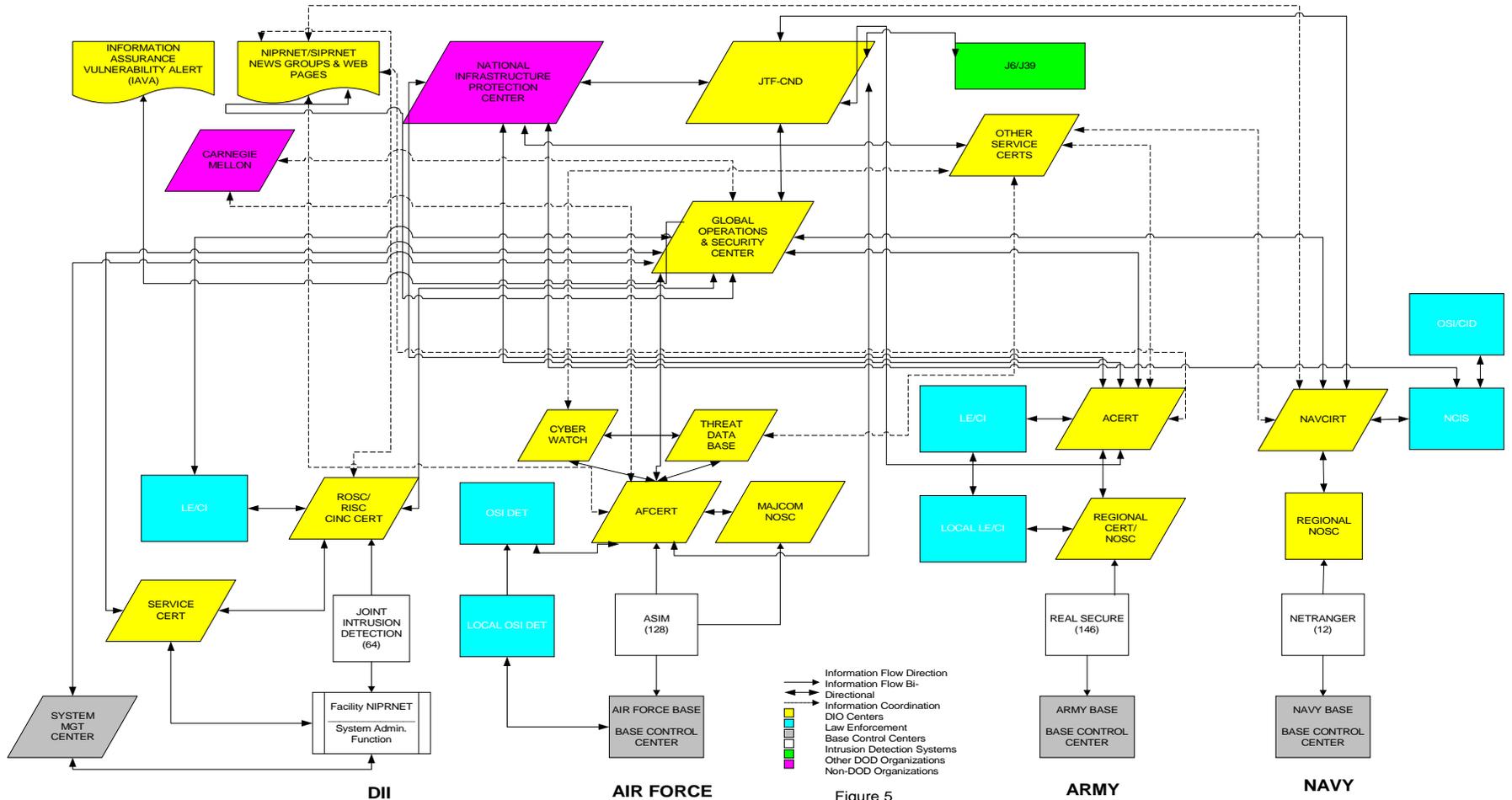


Figure 5



Preliminary Observations

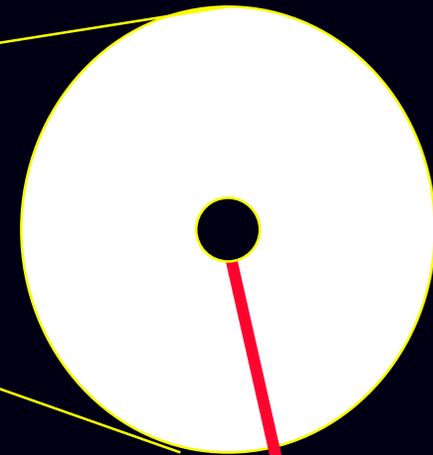
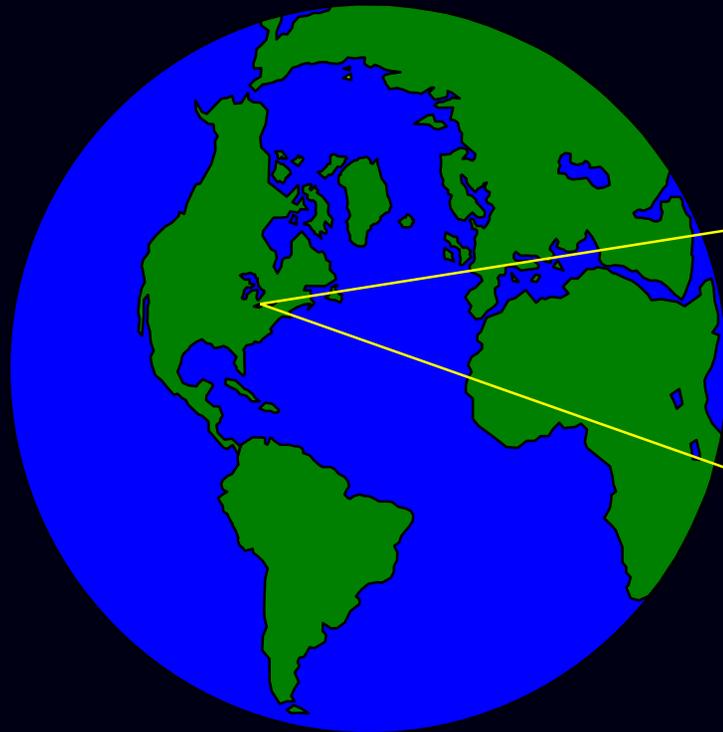
Some high-level general observations have been identified in the following areas

- Network Monitoring*
- Tools*
- Databases*
- Staffing*
- Organizational*
- Information Sharing*
- Policy*
- Classification Guidelines*

Defense-Wide Information Assurance Program



Outsider



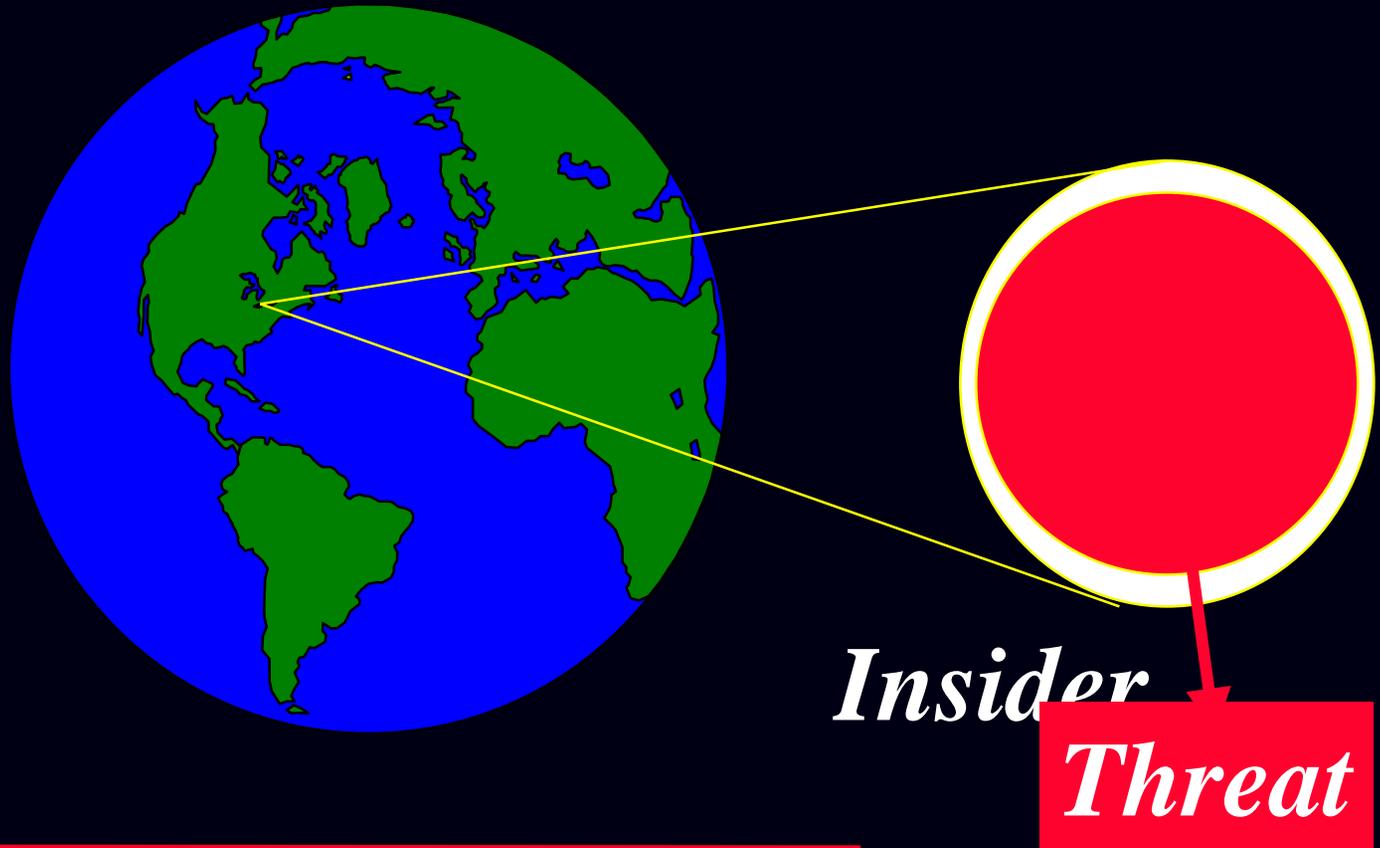
Insider

Threat

Defense-Wide Information Assurance Program



Information Systems Changed the Threat



Defense-Wide Information Assurance Program



Computer Crime Scene - The 9 Recommended Steps

- 1. Contact Law Enforcement*
- 2. Turn On Audit Trails*
- 3. Begin Keystroke Monitoring*
- 4. Assemble the Incident Management Team*
- 5. Designate an Evidence Custodian*
- 6. Begin Recording Costs Associated w/Incident*
- 7. Make Backups & Print Log Files*
- 8. Document Your Activity*
- 9. Theorize*

Defense-Wide Information Assurance Program



Defense-Wide Computer Crime Workshop

Installation Teams Only

Comprised of: ISSO

*Criminal Investigator
JAG*

*Objective: Develop “Go-To Teams” @
Every Installation*

*Late Spring or Early Summer
Colorado Springs*

Defense-Wide Information Assurance Program



Special Agent Jim Christy
Law Enforcement & Counterintelligence Coordinator

Defense-Wide Information Assurance Program
Assistant Secretary of Defense
Command, Control, Communications, and Intelligence
(ASDC3I/DIAP)

Voice: 703-602-9982, DSN 332-9982

Pager: 800-915-1245

Email: James.Christy@osd.pentagon.mil
