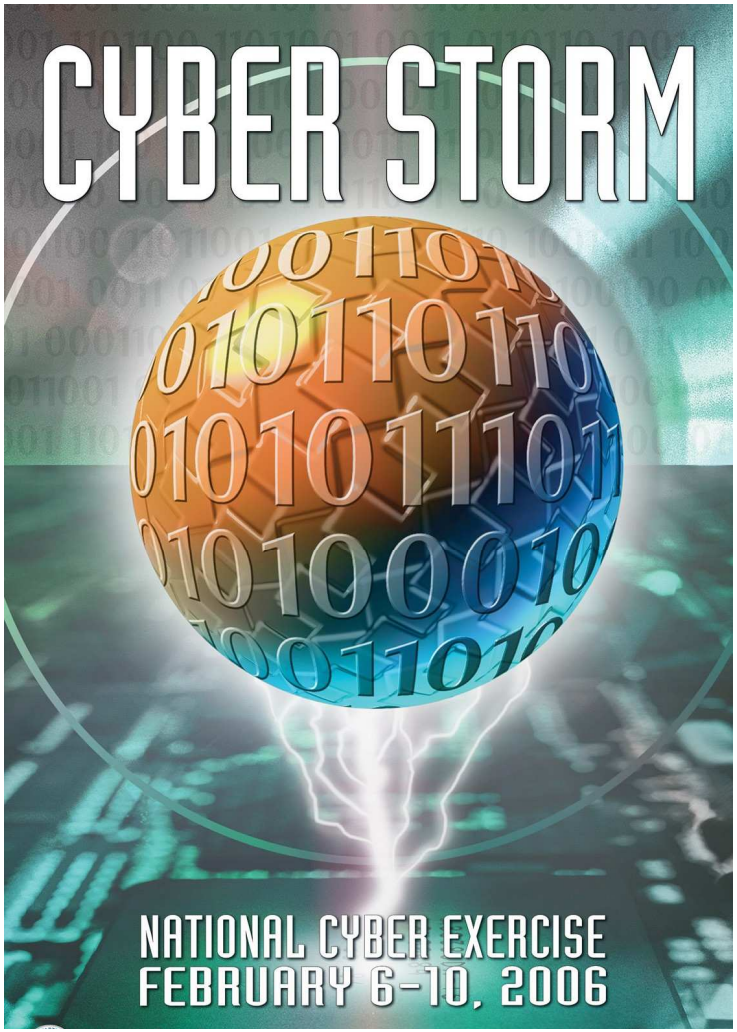
National Cyber Exercise: Cyber Storm

National Cyber Security Division

New York City Metro ISSA Meeting

June 21, 2006



Homeland Security

Agenda

Cyber Storm Overview

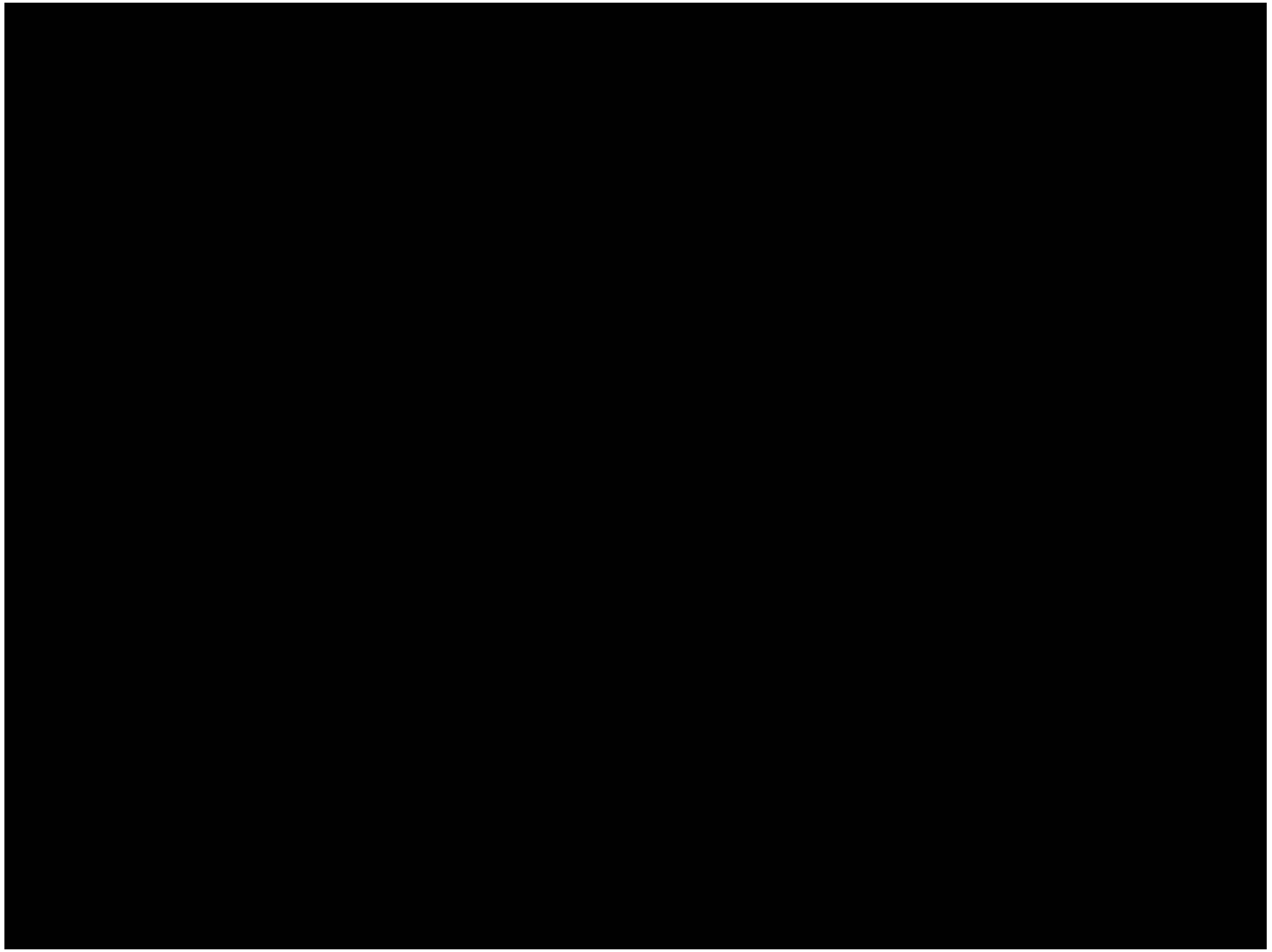
- Exercise Objectives
- Exercise Construct
- Player Universe
- Scenario Context and Scope
- Scenario and Adversary
- Scope and Scale

Overarching Lessons Learned

Way Ahead Cyber Storm II

Homeland Security

Cyber Storm



Cyber Storm Overview

- **What:**
  - **Provided a controlled environment to exercise State, Federal, International, and Private Sector response to a cyber related incident of national significance**
  - **Large scale exercise through simulated incident reporting only – no actual impact or attacks on live networks**
  - **Specifically directed by Congress in FY05 appropriations language and coordinated with DHS National Exercise Program**
- **Who: 300+ participants from**
  - **Federal D/As: Support and/or participation by 8 Departments and 3 Agencies**
  - **States: Michigan, Montana, New York, *Washington (Exercise Control)***
  - **International: Australia, Canada, New Zealand, UK**
  - **Private Sector**
    - **IT: 9 major IT firms**
    - **Energy: 6 electric utility firms (generation, transmission & grid operations)**
    - **Airlines: 2 major air carriers**
    - **ISACs: Multi-State, IT, Energy, *Finance (off the record participant)***
      (Nebraska, North Carolina, South Carolina, Texas @ MS-ISAC)
- **When: February 6-10, 2006**
- **Where: distributed participation from ~ 60 locations including US, Canada, and UK**

Homeland Security

Exercise Objectives

- **Exercise the national cyber incident response community with a focus on:**
  - Interagency coordination under the Cyber Annex to the National Response Plan:
    - Interagency Incident Management Group (IIMG)
    - National Cyber Response Coordination Group (NCRCG)
  - Intergovernmental coordination and incident response:
    - Domestic: State – Federal
    - International: Australia, Canada, NZ, UK & US
  - Identification and improvement of public-private collaboration, procedures and processes
  - Identification of policies/issues that affect cyber response & recovery
  - Identification of critical information sharing paths and mechanisms
- **Raise awareness of the economic and national security impacts associated with a significant cyber incident**

Homeland Security

Exercise Construct

Feb. 6	Feb. 7	Feb. 8	Feb. 9	Feb. 10
Build-Up [D-300 - D-14]	Build-Up [D-7&D-1]	Crisis Phase [D Day]	Response & Recovery [D+1]	Response & Recovery [D+5-7]
Mon. 4 hrs	Tue. 8 hrs	Wed.-Thurs. 36 hrs		Fri. 4 hrs

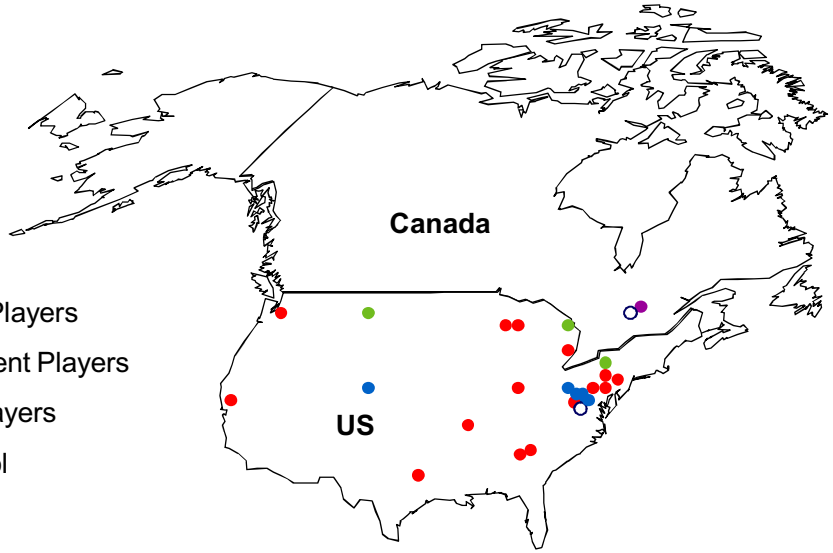
State Prep

Live Play

State Play & Hotwash

TTX & Hotwash

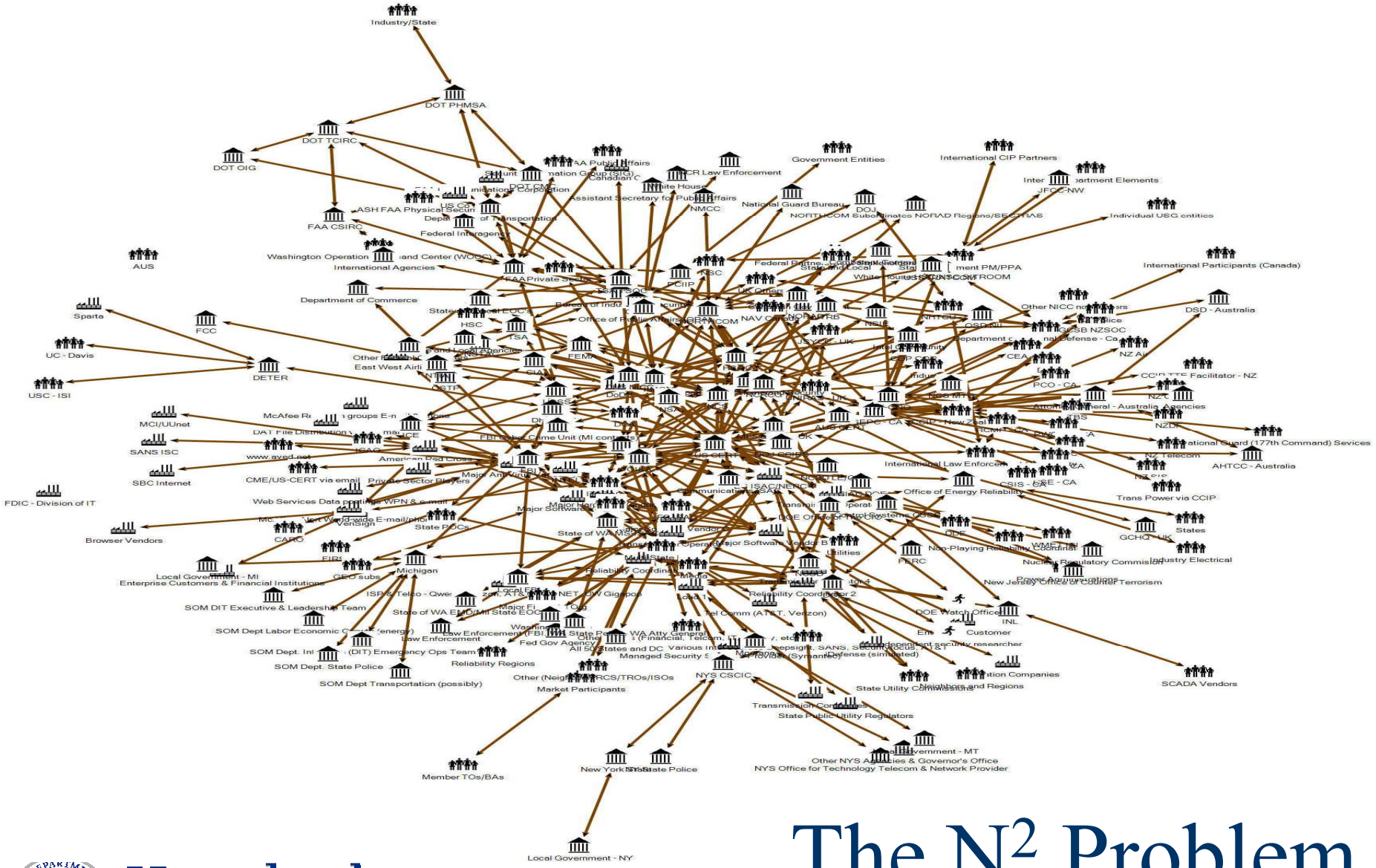
Aus & NZ TTXs Thurs



- Federal Players
- Private Sector Players
- State Government Players
- International Players
- Exercise Control

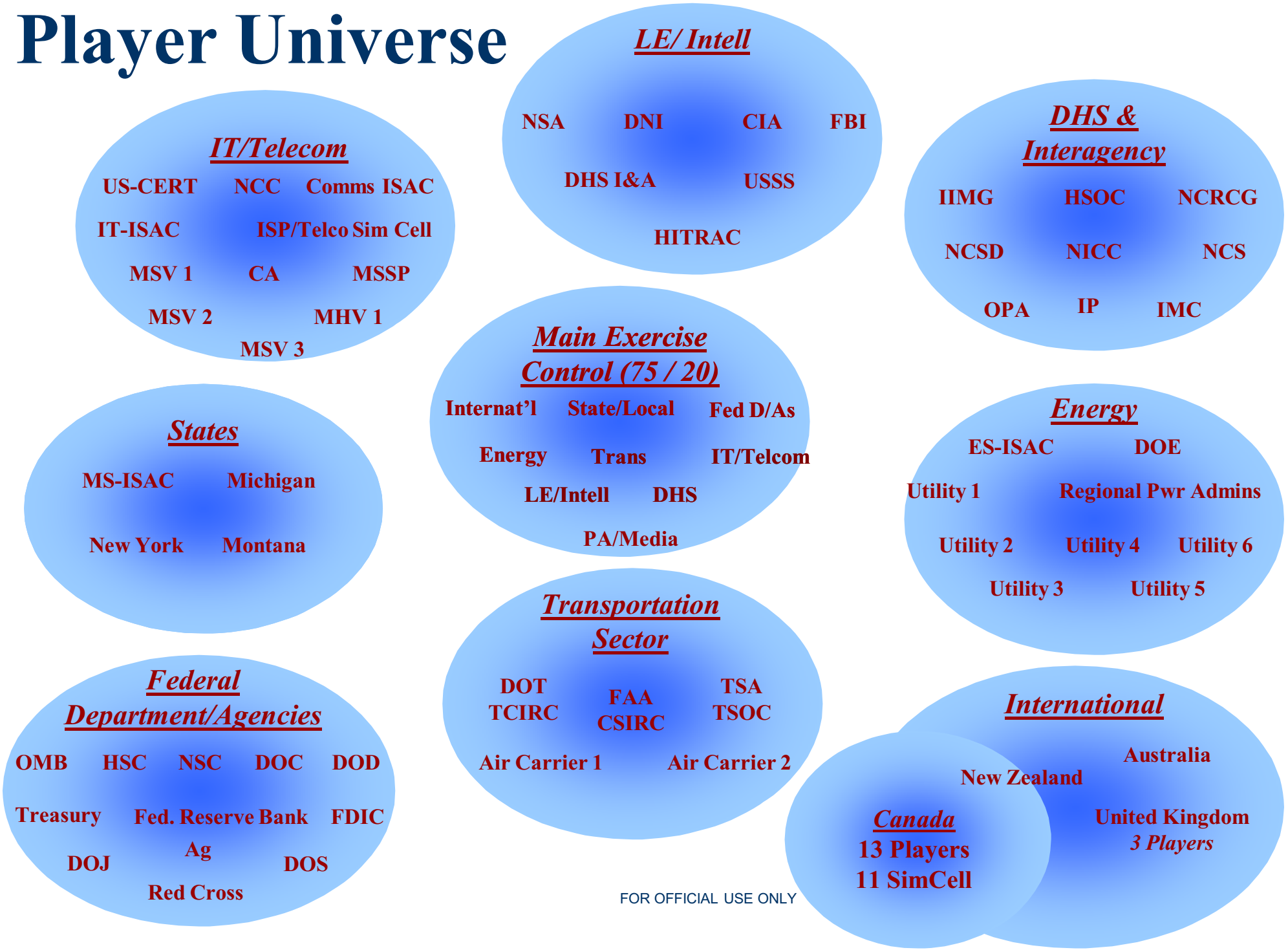
Homeland Security

Cyber Storm Player Universe



The N² Problem

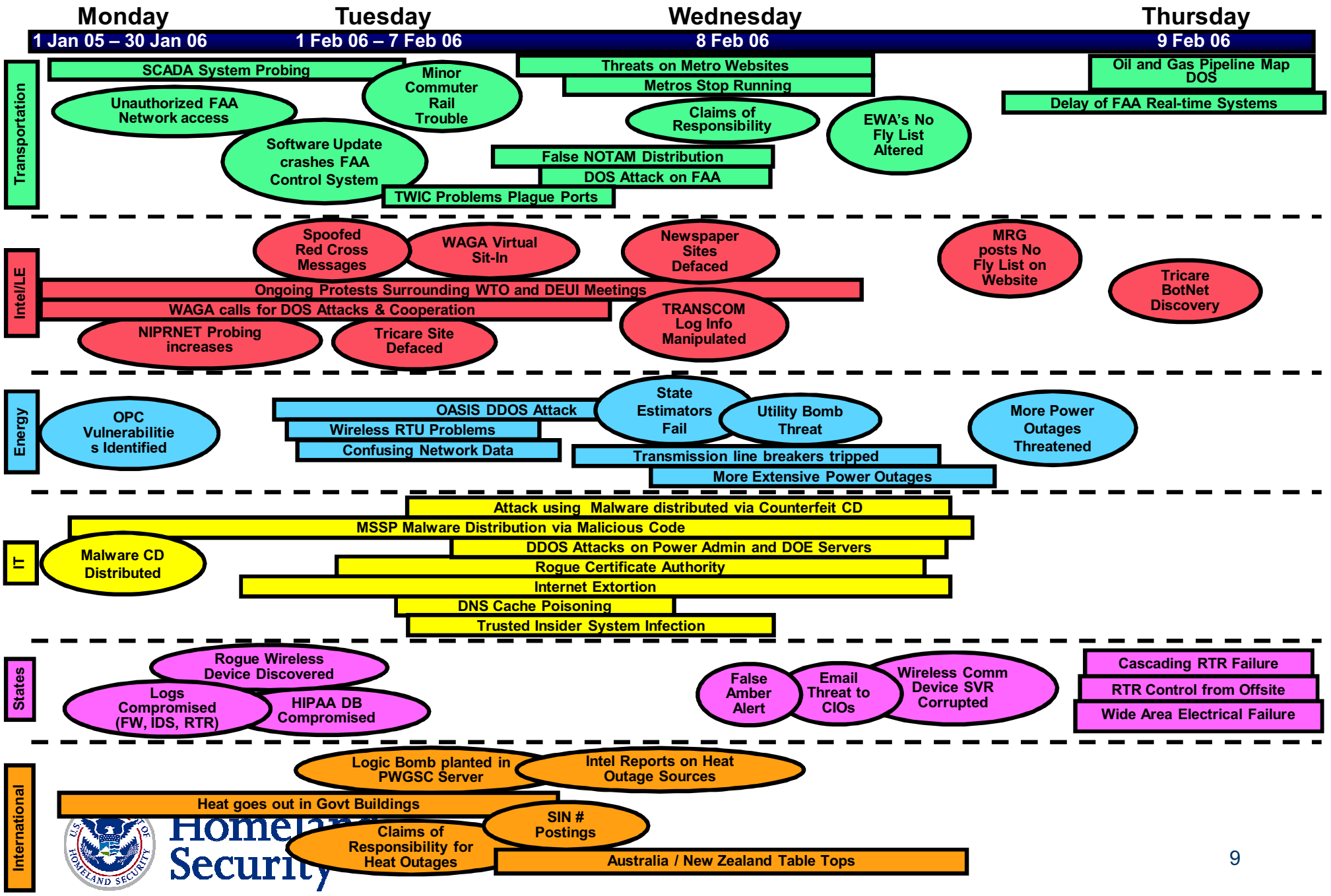
Player Universe



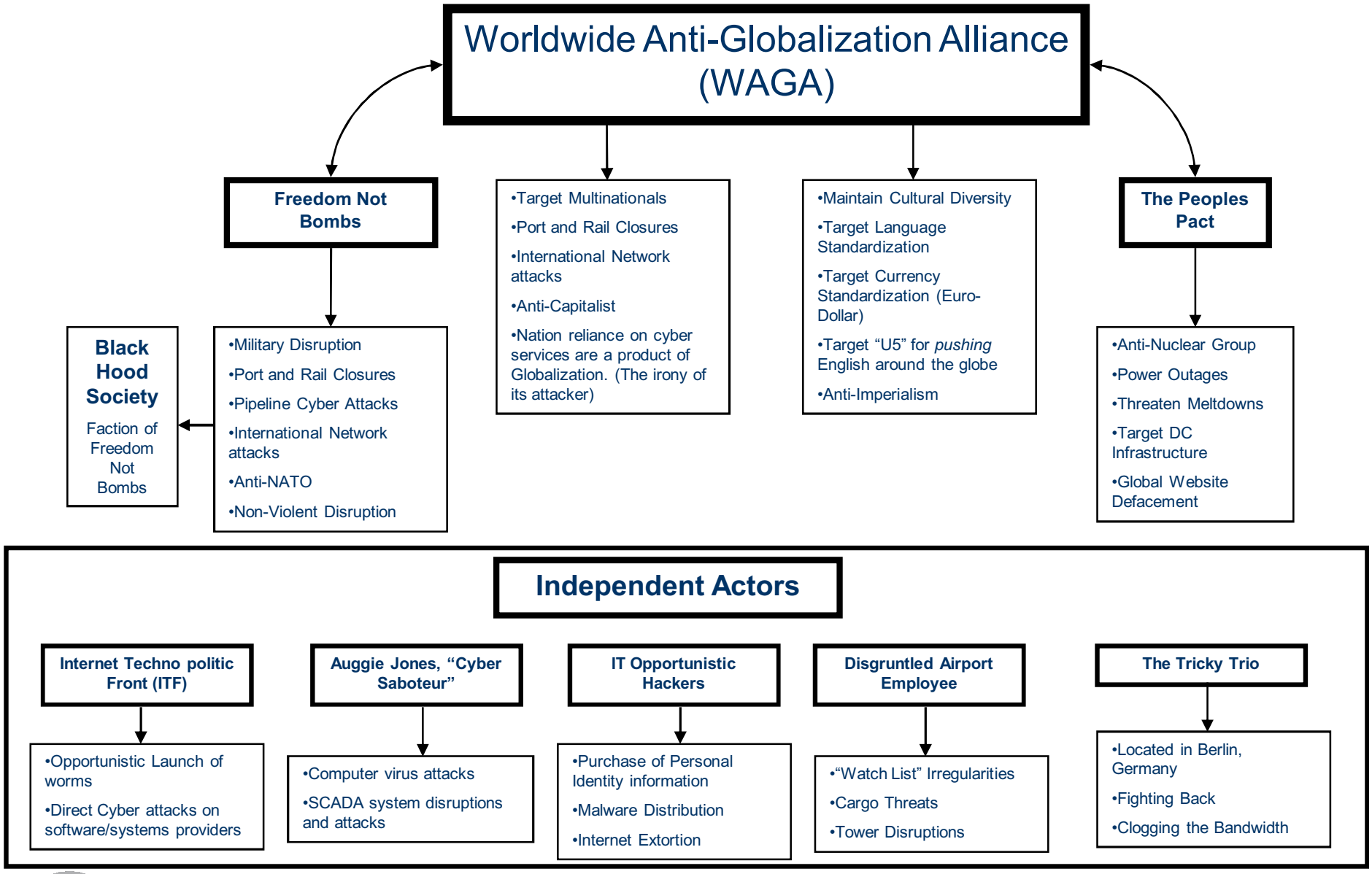
Scenario Context and Scope

- **A simulated large-scale cyber incident affecting Energy, Information Technology (IT), Telecommunications and Transportation infrastructure sectors.**
- **Cyber Storm scenario included:**
  - **Cyber attacks through control systems, networks, software, and social engineering to disrupt transportation and energy infrastructure elements**
  - **Cyber attacks targeted at the IT infrastructure of State, US Federal and International Government agencies intended to:**
    - **degrade government operations/delivery of public services**
    - **diminish the ability to remediate impacts on other infrastructure sectors**
    - **undermine public confidence**
- **The exercise was NOT focused on the consequence management of the physical infrastructures affected by the attacks**
  - **Physical consequence management aspects largely provided to players via robust Exercise Control cell**

Scenario Timeline by Thread



Adversary


Worldwide Anti-Globalization Alliance (WAGA)
Freedom Not Bombs
•Target Multinationals
•Port and Rail Closures
•International Network attacks
•Anti-Capitalist
•Nation reliance on cyber services are a product of Globalization. (The irony of its attacker)
•Maintain Cultural Diversity
•Target Language Standardization
•Target Currency Standardization (Euro-Dollar)
•Target "U5" for *pushing* English around the globe
•Anti-Imperialism
The Peoples Pact
Black Hood Society
Faction of Freedom Not Bombs
•Military Disruption
•Port and Rail Closures
•Pipeline Cyber Attacks
•International Network attacks
•Anti-NATO
•Non-Violent Disruption
•Anti-Nuclear Group
•Power Outages
•Threaten Meltdowns
•Target DC Infrastructure
•Global Website Defacement
Independent Actors
Internet Techno politic Front (ITF)
•Opportunistic Launch of worms
•Direct Cyber attacks on software/systems providers
Auggie Jones, "Cyber Saboteur"
•Computer virus attacks
•SCADA system disruptions and attacks
IT Opportunistic Hackers
•Purchase of Personal Identity information
•Malware Distribution
•Internet Extortion
Disgruntled Airport Employee
•"Watch List" Irregularities
•Cargo Threats
•Tower Disruptions
The Tricky Trio
•Located in Berlin, Germany
•Fighting Back
•Clogging the Bandwidth

Scenario Timeline Thread/Villain

WAGA
Black Hood Society
People's Pact
ITF
Tricky Trio
BBB
MRG
Disgruntled Employee
DOWN
Independent Actor

Monday	Tuesday	Wednesday	Thursday
1 Jan 05 – 30 Jan 06	1 Feb 06 & 7 Feb 06	8 Feb 06	9 Feb 06

Transportation

- SCADA System Probing
- Unauthorized FAA Network access
- Minor Commuter Rail Trouble
- Software Update crashes FAA Control System
- Threats on Metro Websites
- Metros Stop Running
- Claims of Responsibility
- EWA's No Fly List Altered
- False NOTAM Distribution
- DOS Attack on FAA
- Wardial attack on AFSS
- Oil and Gas Pipeline Map DOS
- Delay of FAA Realtime Systems

Intel/LE

- Spoofed Red Cross Messages
- WAGA Virtual Sit-In
- Newspaper Sites Defaced
- Ongoing Protests Surrounding WTO and DEUI Meetings
- WAGA calls for DOS Attacks & Cooperation
- NIPRnet Probing increases
- MyPay Balances Zeroed
- Tricare Site Defaced
- NORTHCOM Comm System Info Manipulated
- MRG posts No Fly List on Website
- Tricare BotNet Discovery

Energy

- OPC Vulnerabilities Identified
- OASIS DDOS Attack
- Wireless RTU Problems
- Confusing Network Data
- State Estimators Fail
- Utility Bomb Threat
- Transmission line breakers tripped
- More Extensive Power Outages
- More Power Outages Threatened

IT

- Malware CD Distributed
- Attack using Malware distributed via Counterfeit CD
- MSSP Malware Distribution via Malicious Code
- DDOS Attacks on Power Admin and DOE Servers
- Rogue Certificate Authority
- Internet Extortion
- DNS Cache Poisoning
- New SSL Vulnerability Discovered
- Trusted Insider System Infection

States

- Rogue Wireless Device Discovered
- Logs Compromised (FW, IDS, RTR)
- HIPAA DB Compromised
- False Amber Alert
- Email Threat to CIOs
- Wireless Comm Device SVR Corrupted
- Cascading RTR Failure
- RTR Control from Offsite
- Internet Connectivity Losses

International

- Logic Bomb planted in PWGSC Server
- Intel Reports on Heat Outage Sources
- Heat goes out in Govt Buildings
- SIN # Postings
- Claims of Responsibility for Heat Outages
- Australia / New Zealand Table Tops

WAGA Associates
WAGA Sympathizers

Scope and Scale

- **Planning: 18 months**
  - 5 major planning conferences
  - 100-150 participants @ each
  - 5 AAR conferences
- **ExCon: ~100**
  - Exercise network & workstations
  - NXMSEL, web and email servers
  - Simulate media website
  - Hacker websites
  - Physical build
  - Observer group
  - Observation database
- **Players: 300+**
- **Scenario: 800+ injects**
- **Player emails: 21,000+ captured**
- **Cost: $$**
- **Exercise Management Team: peaked @ ~20 FTEs**

Overarching Lessons Learned

- **Correlation of multiple incidents is challenging at all levels:**
  - **Within enterprises / organizations**
  - **Across critical infrastructure sectors**
  - **Between states, federal agencies and countries**
  - **Bridging public – private sector divide**
- **Communication provides the foundation for response**
  - **Processes and procedures must address communication protocols, means and methods**
- **Collaboration on vulnerabilities is rapidly becoming required**
  - **Reliance on information systems for situational awareness, process controls and communications means that infrastructures cannot operate in a vacuum**
- **Coordination of response is time critical**
  - **Cross-sector touch points, key organizations, and SOPs must be worked out in advance**
  - **Coordination between public-private sectors must include well articulated roles and responsibilities**

Overarching Lessons Learned

- **Strategic Communications / Public Messaging**
  - Critical part of government response that should be coordinated with partners at all levels
- **Policy Coordination**
  - Senior leadership / interagency bodies should develop more structured communication paths with international counterparts
  - Strategic situational awareness picture cannot be built from a wholly federal or domestic perspective in the cyber realm
- **Operational Cooperation**
  - True situational awareness will always include an external component
  - Initial efforts at international cooperation during CS provided concrete insights into of near term development of way ahead for ops/tech info sharing
  - Communication paths, methods, means and protocols must be solidified in advance of crisis/incident response
    - Who do I call? When do I call? How do I call them?
    - Secure and assured communications are critical in order to share sensitive information
  - Cooperation must include ability to link into or share info in all streams: e.g., Cyber, Physical, LE, Intelligence

Way Ahead– Cyber Storm II

- Tentatively scheduled for March 2008
- Fall 2006, DHS and key stakeholders will begin development of CSII overall concept and scenario focus
- Spring 2007, CSII CONOPS will be finalized
- Based on the scenario focus areas, DHS will coordinate with the sector specific agencies and the relevant Information Sharing Analysis Centers and Private Sector Coordinating Councils (NIPP) for individual private sector participants.

Homeland Security