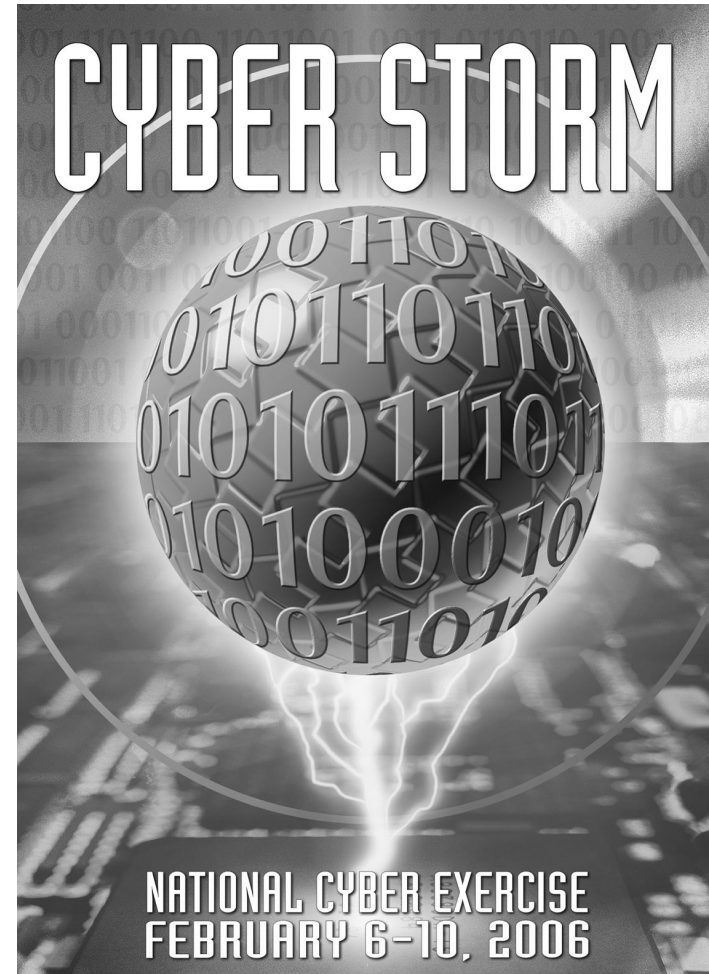


National Cyber Exercise: Cyber Storm

National Cyber Security Division

New York City Metro ISSA Meeting

June 21, 2006



This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

Agenda

Cyber Storm Overview

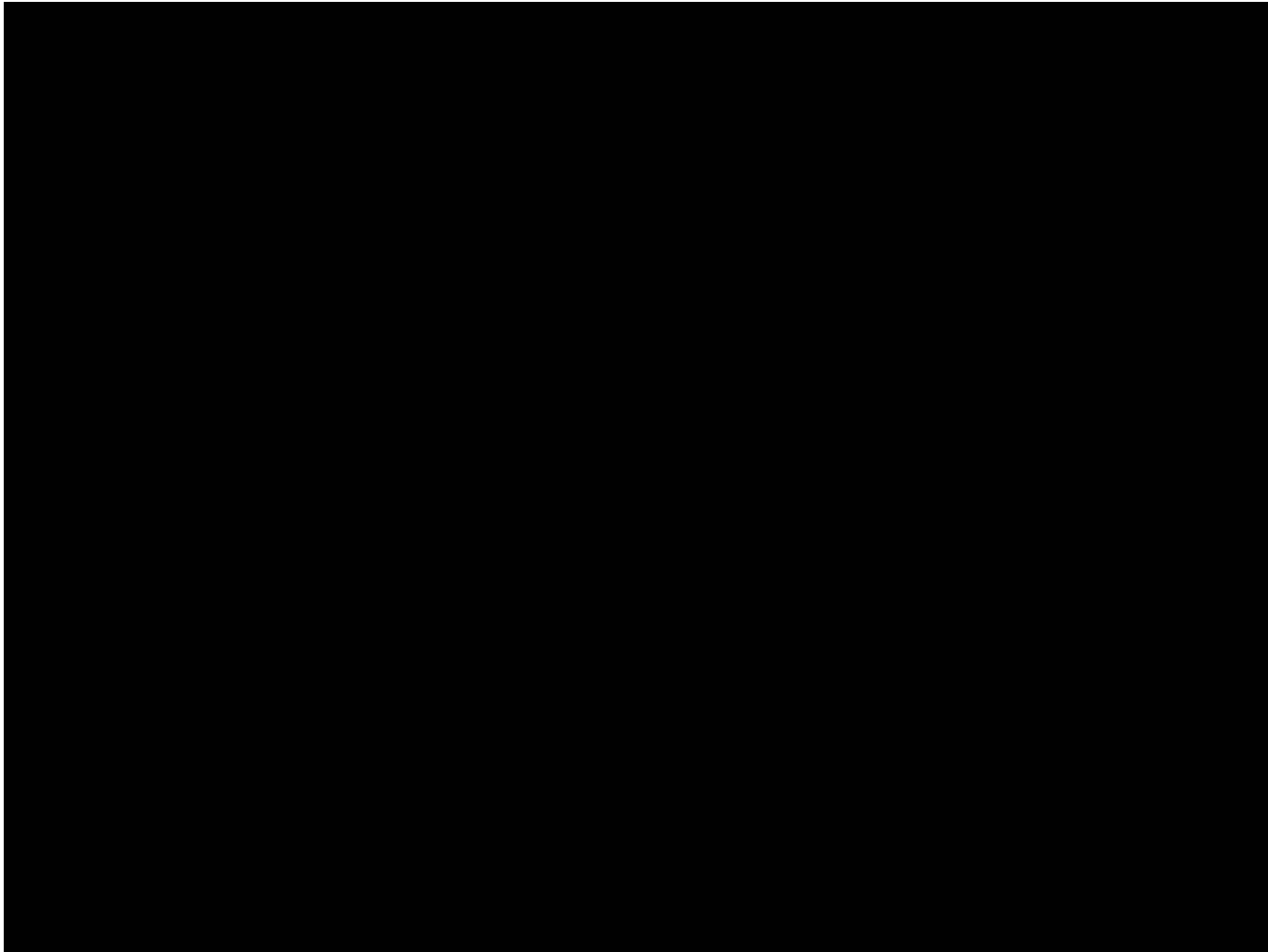
- Exercise Objectives
- Exercise Construct
- Player Universe
- Scenario Context and Scope
- Scenario and Adversary
- Scope and Scale

Overarching Lessons Learned

Way Ahead Cyber Storm II



Cyber Storm



FOR OFFICIAL USE ONLY

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

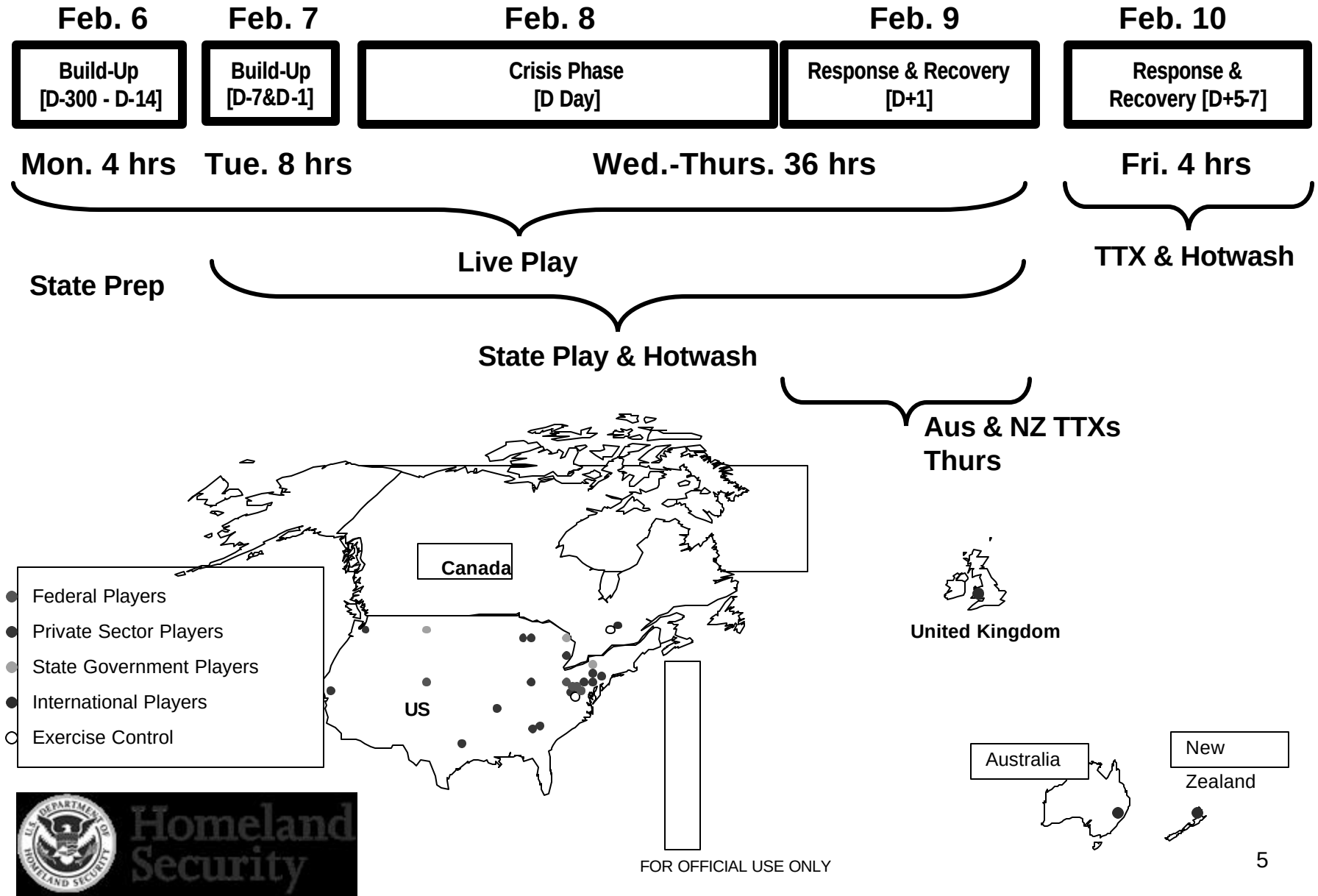


Exercise Objectives

- ▶ **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**



Exercise Construct



U.S. DEPARTMENT OF
HOMELAND SECURITY



Player Universe

IT/Telecom

US-CERT NCC Comms ISAC
IT-ISAC ISP/Telco Sim Cell
MSV 1 CA MSSP
MSV 2 MHV 1
MSV 3

LE/ Intell

NSA DNI CIA FBI
DHS I&A USSS
HITRAC

DHS & Interagency

IIMG HSOC NCRCG
NCSD NICC NCS
OPA IP IMC

States

MS-ISAC Michigan
New York Montana

Main Exercise Control (75 / 20)

Internat'l State/Local Fed D/As
Energy Trans IT/Telcom
LE/Intell DHS
PA/Media

Energy

ES-ISAC DOE
Utility 1 Regional Pwr Admins
Utility 2 Utility 4 Utility 6
Utility 3 Utility 5

Federal

Department/Agencies

OMB HSC NSC DOC DOD
Treasury Fed. Reserve Bank FDIC
DOJ Ag DOS
Red Cross

Transportation Sector

DOT FAA TSA
TCIRC CSIRC TSOC
Air Carrier 1 Air Carrier 2

International

Canada
13 Players
11 SimCell

Australia
New Zealand
United Kingdom
3 Players

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**



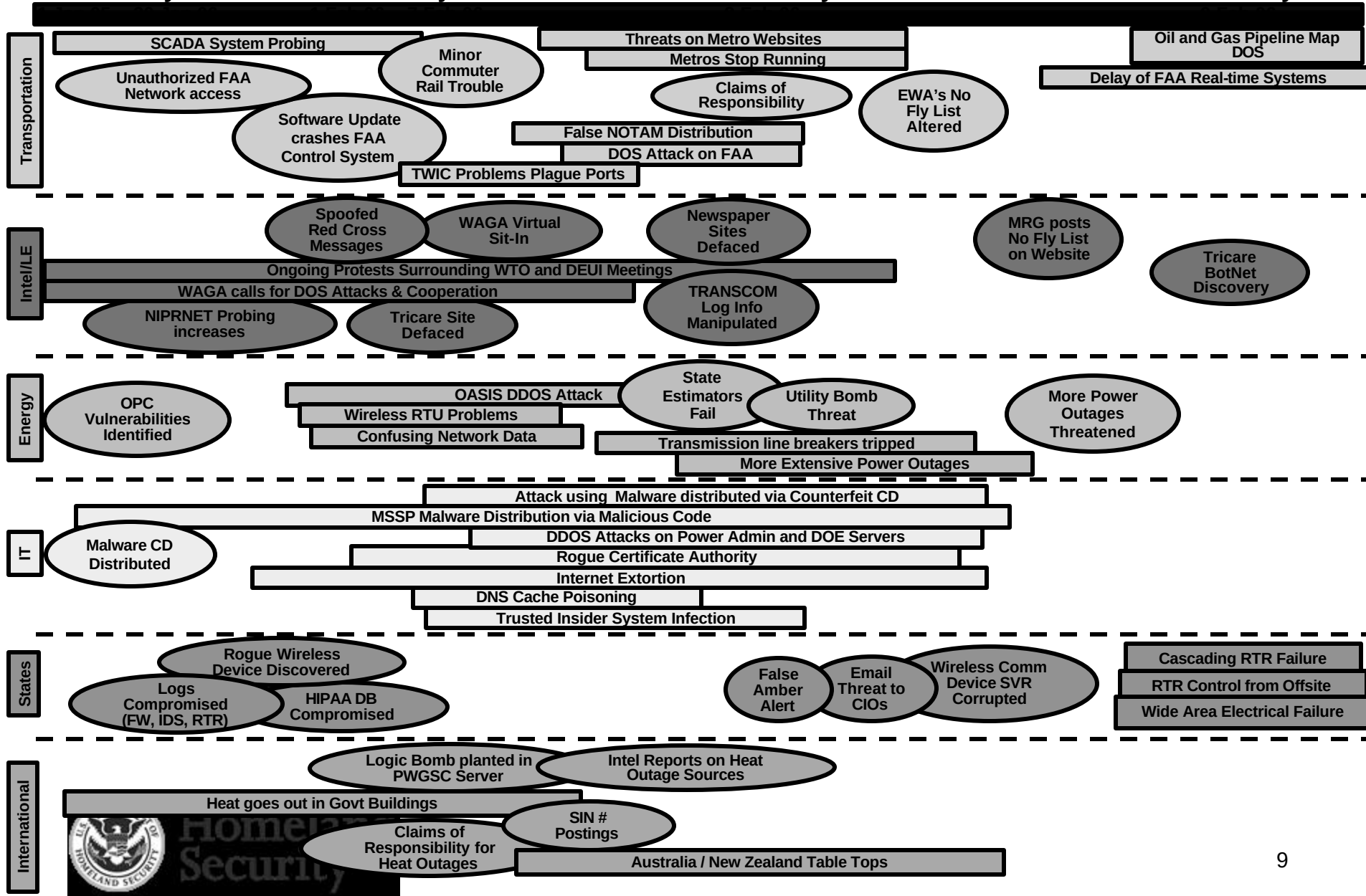
Scenario Timeline by Thread

Monday

Tuesday

Wednesday

Thursday



Adversary

Worldwide Anti-Globalization Alliance (WAGA)

Freedom Not Bombs

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

- 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

- 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



Homeland Security

Scenario Timeline Thread/Villain

- WAGA

Black Hood Society

People's Pact

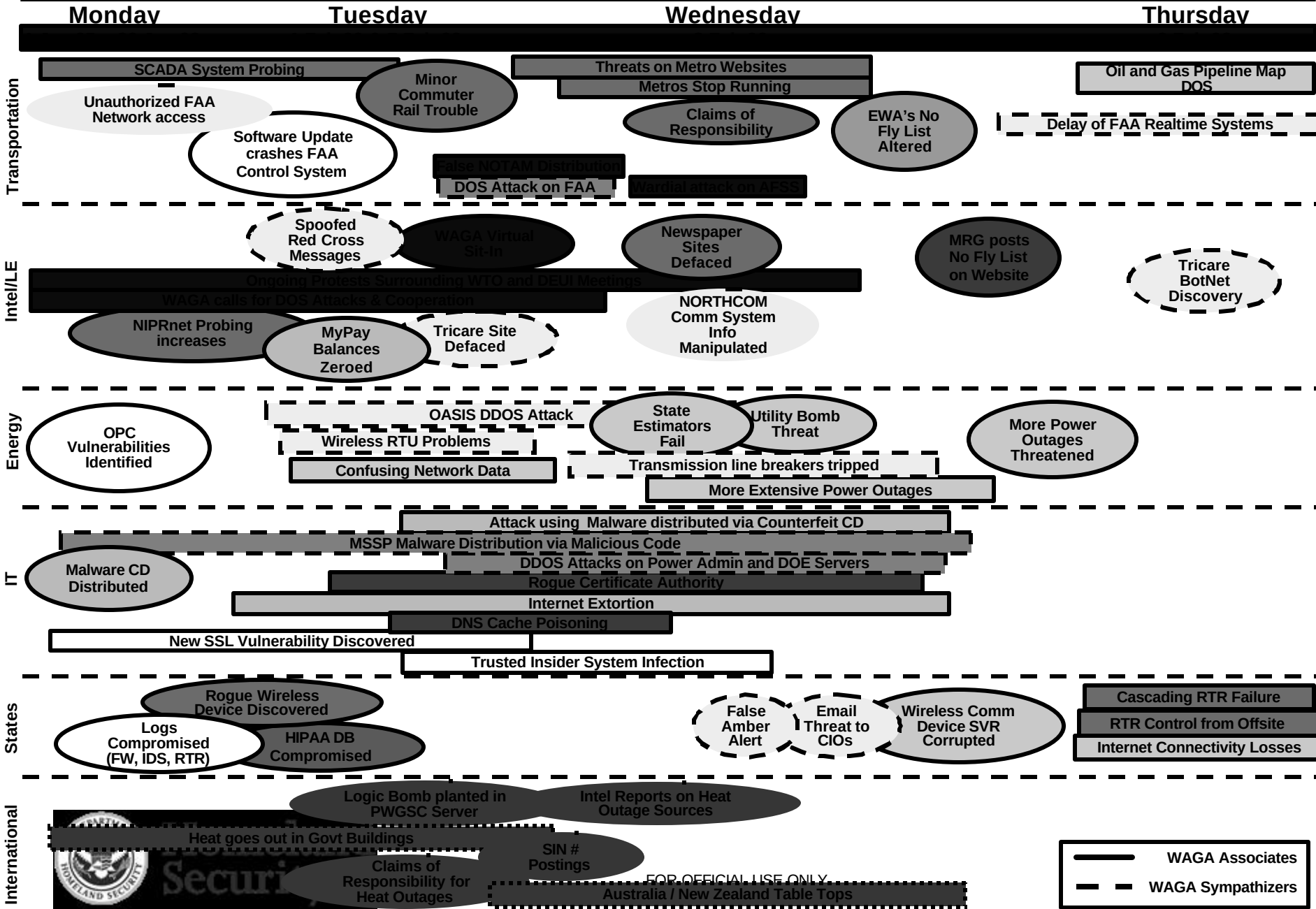
ITF
- Tricky Trio

BBB

MRG
- Disgruntled Employee

DOWN

Independent Actor



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