Iranian Attack Statistics

(b)(1) USSC

ATTACK STATISTICS

(b)(1) USSC

(b)(1)

USCYBERCOM

Team Cyber Update (Iran)

14 March 2013

The overall classification of this briefing is: ~~TOP SECRET//~~(b)(1)~~//NOFORN~~

Classified By: alperpe
Derived From: USCYBERCOM SCG
Dated: 20111011
Declassify On: 20370801

Team Cyber Updates

Military C2

(b)(1) USSC

Anti-Access

(b)(1) USSC

Team Cyber Updates

(b)(1) USSC

Team Cyber Updates

(b)(1) USSC

Iranian Cybersecurity Threats

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC Planning

- (U)Limited Scope (b)(1) USSC
  - (S//REL USA, FVEY) (b)(1) USSC
    (b)(1) USSC
  - (TS/(b)(1)/REL USA, FVEY) (b)(1) USSC
    (b)(1) USSC
    - (b)(1) USSC
    -
  - (U) NSS and JS are currently (b)(1) USSC with Inter Agency.
  - (TS//REL USA, FVEY) (b)(1) USSC
  - (TS//REL USA, FVEY) (b)(1) USSC
    (b)(1) USSC
- (U) Malware
  - (TS/(b)(1)/REL USA, FVEY) (b)(1) USSC
    (b)(1) USSC
  - (S//REL USA, FVEY) (b)(1) USSC
    (b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

Questions

Congress Storyboard

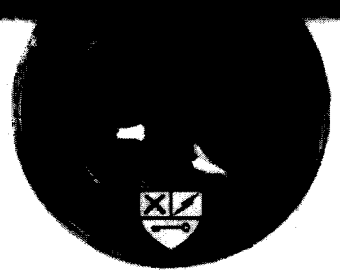
Draft v22

The overall classification of this briefing is: ~~TOP SECRET~~ (b)(1) ~~//NOFORN~~

Classified By: ecrocke
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371201

Agenda

- Adversary Activity and Capabilities
- How the Adversary Fights
- How We Fight
- Cyber Forces We Need for the Fight
- Maintaining Our Strategic Advantage



Adversary Activity and Capabilities

Overview of Adversary Activity DRAFT

(b)(1) USSC

U.S. NETWORKS

CNE, CNA capabilities & unknown activity

(b)(1) USSC

(b)(1) USSC

(S//REL) (b)(1) USSC

(b)(1) USSC

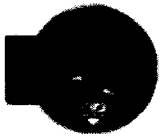
(b)(1) USSC

Graphic: (TS//(b)(1))

~~TOP SECRET~~ (b)(1) ~~REL TO USA, FVEY~~

(b)(1) USSC

(b)(1) USSC



(b)(1) USSC

- (b)(1) USSC

(b)(1) USSC

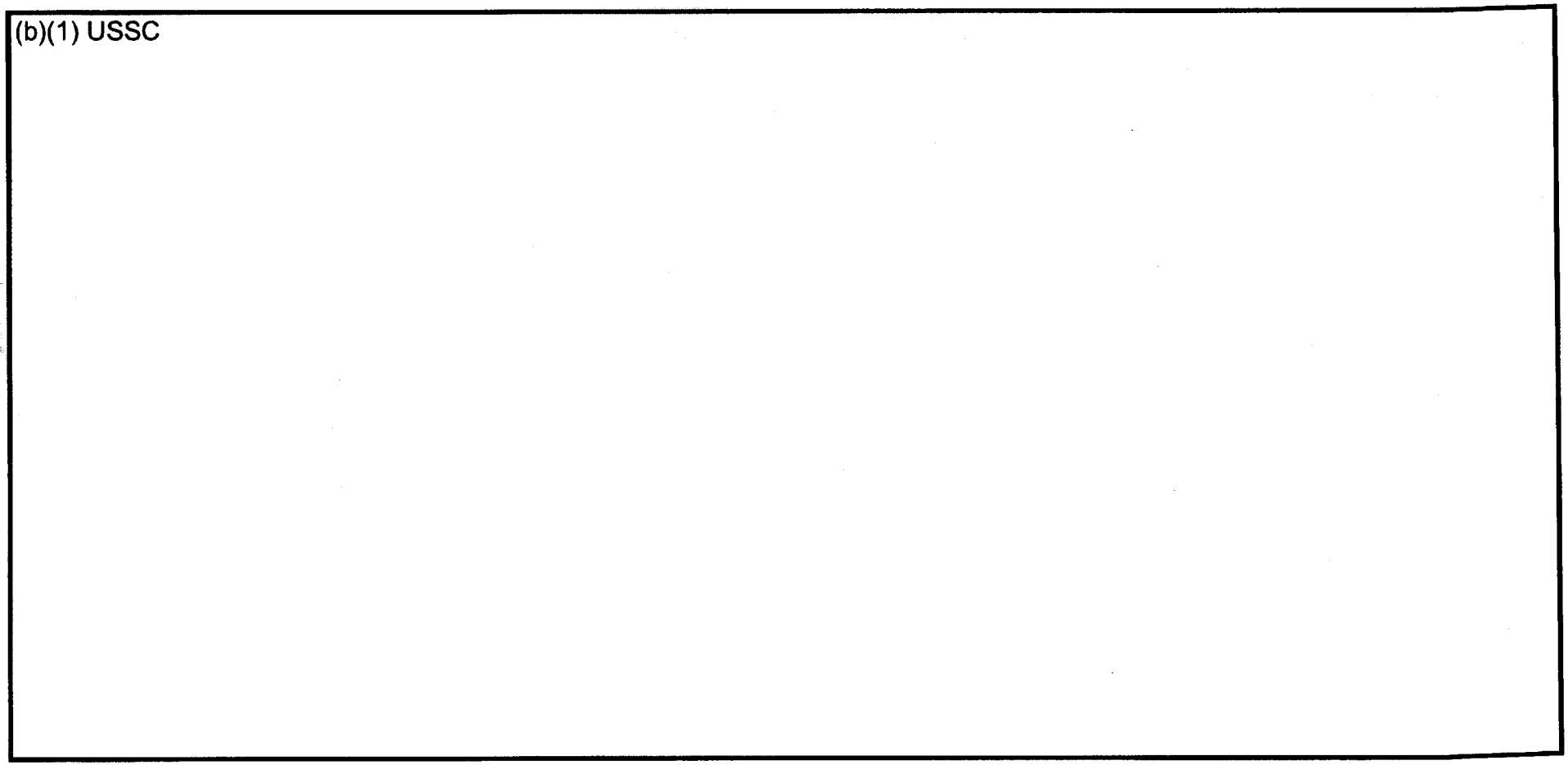
(b)(1) USSC

How The Adversary Fights

The Anatomy of a DDoS Attack

(b)(1) USSC

Key Terrain of the Fight



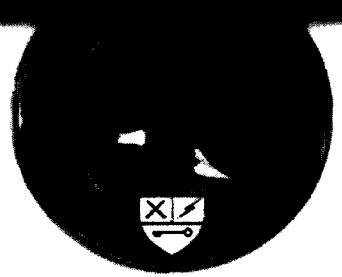
How We Fight

(U) Cyber Options Against Key Terrain

(b)(1) USSC

Force on Force – National Mission Fight

(b)(1) USSC



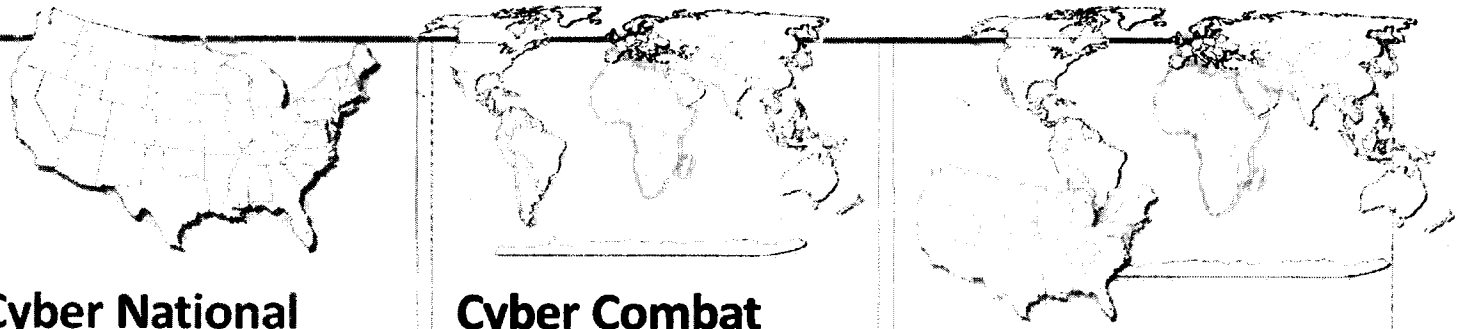
Cyber Forces We Need for the Fight

Cyber Mission Forces

USCYBERCOM Operational Focus Areas
Supports Lines of Effort

Strategic Defense Against Offensive Cyber Attack
Integration into CCMD Contingency and Operational Plans
Operating and Defending DoD Infrastructure (DODIN)

USCYBERCOM Forces
Trained, certified and operates as a team



Cyber National Mission Forces (CNMF)

*Defend the nation by **Seeing** adversary activity, **Blocking** attacks and **Maneuvering** to defeat them*

Cyber Combat Mission Forces (CCMF)

Conduct military cyber operations in support of combatant commands

Cyber Protection Forces (CPF)

Defend DoD Information Networks (DODIN) and, when authorized, other infrastructure.

NSA Reach Back
Supports CNMF & CNMT

Solves specific operational challenges. Provides high value, low density skill sets.

NSA General Support
Provides support as a whole to USCYBERCOM forces

Global Cryptologic Platform

All teams must be trained in cyber basics to surge to other teams when needed.

Cyber Mission Forces

(b)(1) USSC

(b)(1) USSC

How We Employ Forces Against Key Terrain

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

Maintaining Our Strategic Advantage

(U) We Cannot Fight If We Cannot See

(b)(1) USSC

Logical to Physical (U)

Geolocation of adversary's networks and key nodes, shows relationships between connections in cyber and in physical world

Networks (U)

Enables planning, operations and deconfliction

Geographic Terrain (U)

Critical infrastructure, key actors and key resources

Real-Time Visibility (U)

Networks, adversary attacks, C2 nodes, botnets

(b)(1) USSC **(S//REL)**

(b)(1) USSC

We Must Integrate Missions and Organizations to Meet the Threat

PERSISTANT & GROWING THREAT

Exploitation

- (U) 2007 -Hacking (Oak Ridge National Laboratory)
- (U) 2008 - Hacking into classified networks (Buckshot Yankee)

Disruption

- (U) 2007 – DDoS (Georgia)
- (U) 2010 - Cyber Attack (STUXNET)
- (U) 2011 – Cyber Attack (Nasdaq)
- (U) 2011 – Network Intrusion (RSA)

Destruction

- (U) 2012 Cyber Attack (ARAMCO – 30,000+ computers destroyed)
- (U) 2011-Present DDoS Attacks (Financial Sector)
- (TS/(b)(1)EL) (b)(1) USSC

(b)(1) USSC

INTEGRATION OF MISSIONS & ORGANIZATIONS

Cyber Operations Using (b)(1) USSC

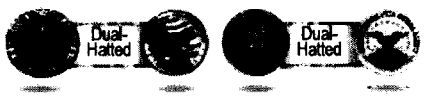
Cyber Military Planning & Offensive OPS

Operating & Defending DoD Networks

Integrated Offense & Defense

2004-2005

JTF-GNO & JFCC-NW established as separate commands



2008

JTF-GNO OPCON to JFCC-NW for control under one Commander

2010

USCYBERCOM Activated as Sub-Unified Command

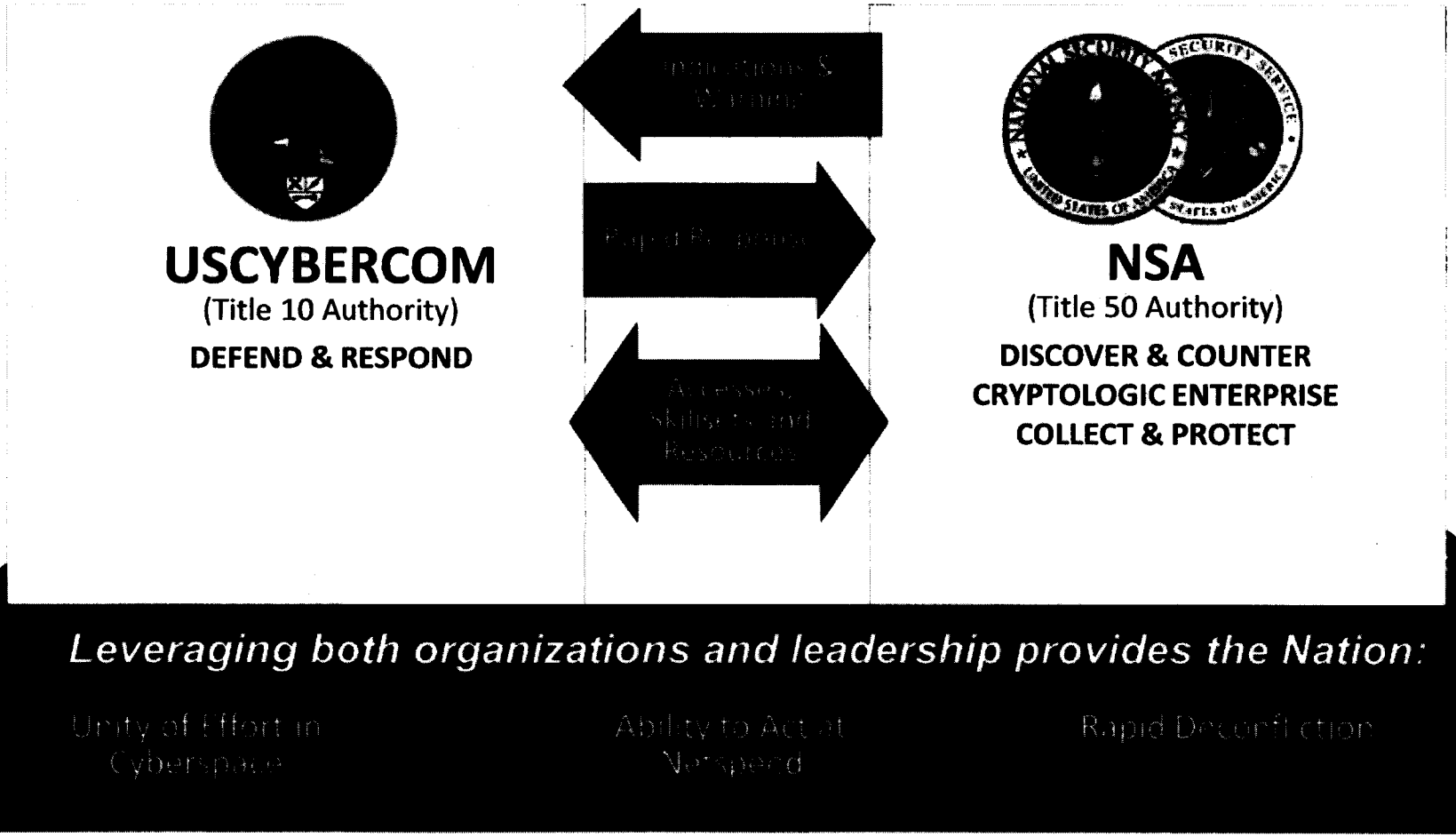
Set Standards for Building, Training & Employing the Force

Identification, Prioritization & Allocation of Cyber Capability Requirements

2013

When directed, USCYBERCOM Activated as Unified Command

We Must Fully Leverage the Capabilities of USCYBERCOM & NSA for the Nation



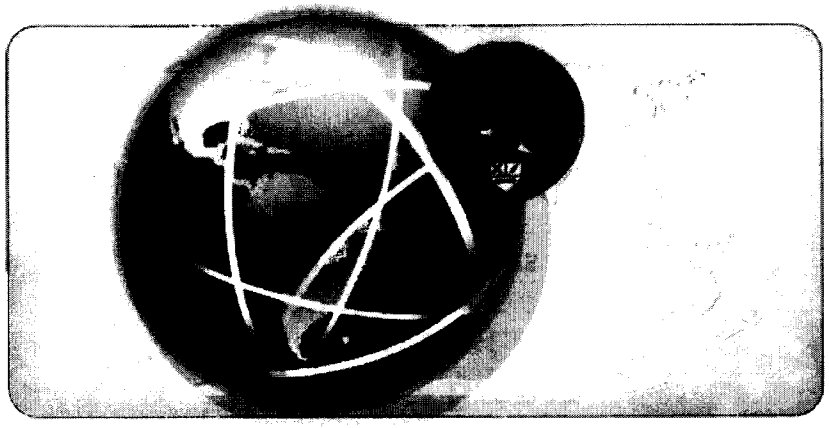
(b)(1) USSC

We Must Synchronize and Deconflict Operations

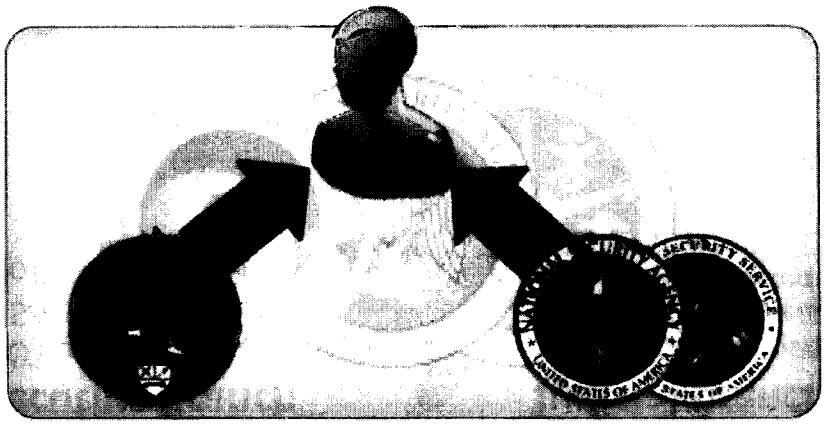
(b)(1) USSC

Ability to Act Enabled by ....

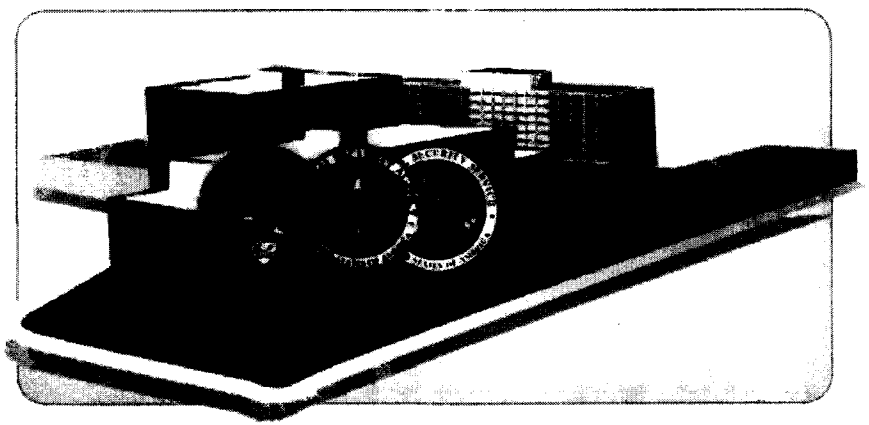
Unified Command



Dual-Hatting of CDR USCYBERCOM and DIRNSA

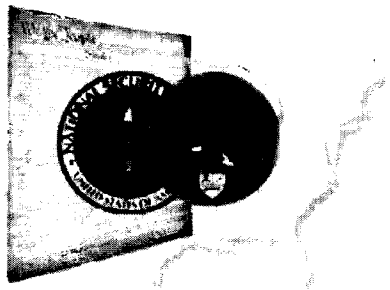


Coordination with Co-Location



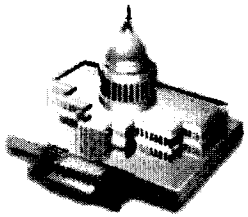
Information Sharing with Private Sector & Protecting Civil Liberties

Oversight and Compliance



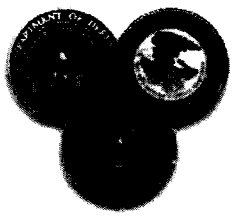
NSA & USCYBERCOM are committed to protecting privacy and civil liberties.

Total Government Approach



Legislative Branch

Key committees:
- Intelligence
- Armed Services
- Judiciary
- Appropriations
- Homeland Security



Executive Branch
- POTUS
- NSA
- DoD
- DNI
- DoJ
- AG

Judicial Branch
- FISA Court: *provides oversight over intelligence activities conducted pursuant to FISA*

Congressional Role

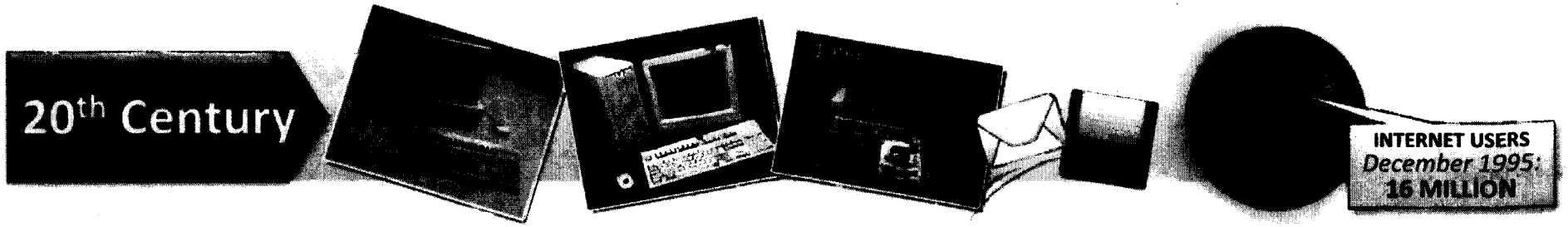
- Oversight and Compliance
- Authorities: Cyber Legislation, FISA Amendment Act (FAA)
- Mission Oversight
- Resourcing

Take Aways

- How USCYBERCOM will maintain strategic advantage in cyberspace:
  - We see the attack (visualization through NSA's world-class cryptologic enterprise)
  - We have adequate number of highly trained cyber forces in place and on net
  - We share the information (legislation to allow real-time sharing with industry)
  - We act swiftly with unity of effort (unified command, dual-hatting, SROE, policy, C2)

Backup

Beyond the Internet toward Cyberspace...



Internet was used for information sharing, research, chatting, instant messaging, emailing...

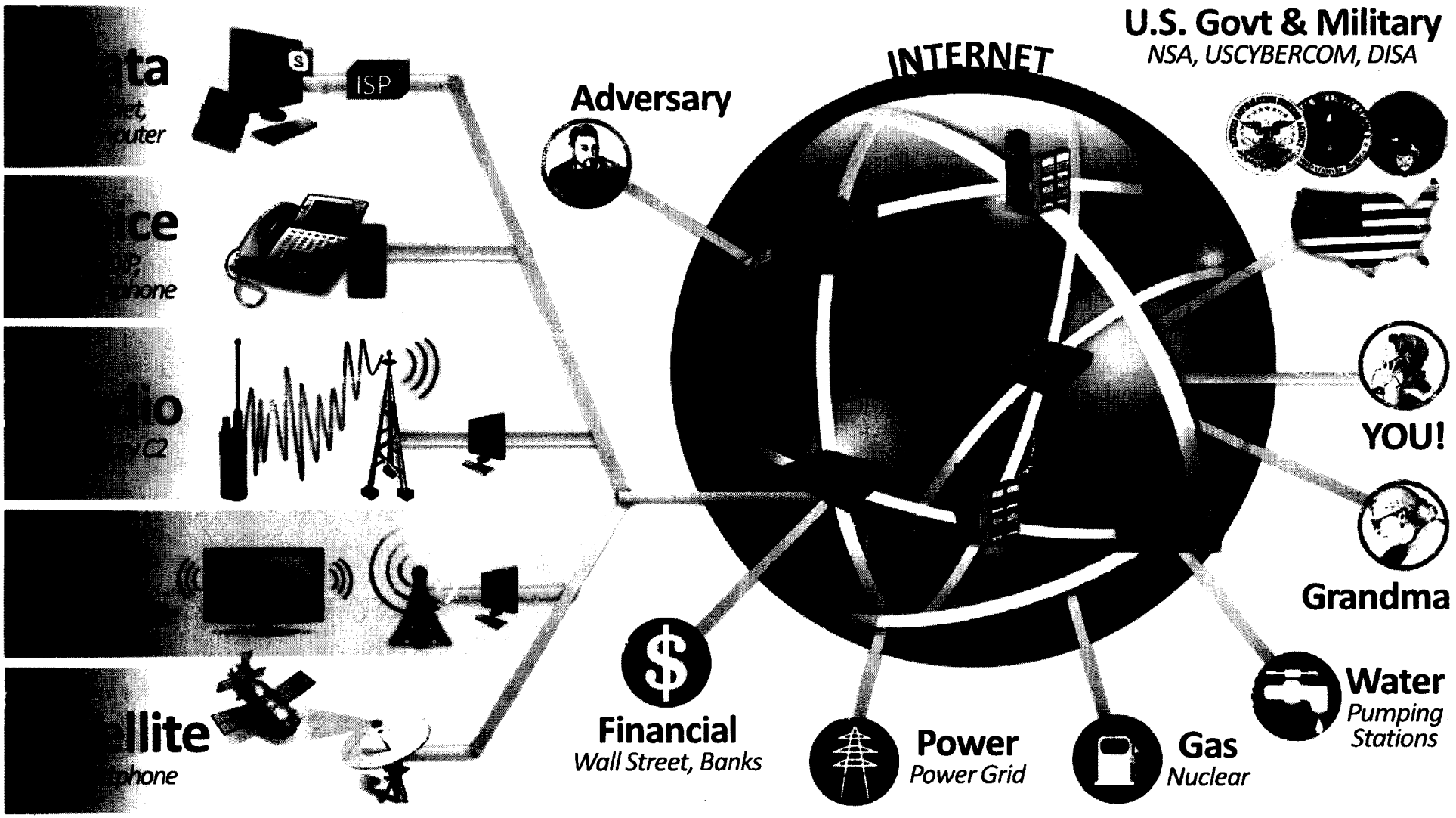
- Slow connection speeds built around stationary computers
- Initial intent was for an open network; security was not a concern

Cyberspace is used for generating and storing information, social networking, shopping, entertainment, communicating, banking, information sharing, emailing, gaming...

- Faster connection speeds built around online servers and storage
- Ability to access information from computers, phones, televisions and even refrigerators! The Internet is at our fingertips
- Security is a concern: increase in spam/spyware/viruses because our wealth and information is on the network
- Cyberspace stores our nation's secrets, bank information and military plans
- Cyberspace is used to operate our power grid, water systems and other critical infrastructure
- Cyberspace is a place for rich personal interactions and information exchanges.

The Same Network

A single network carries our wealth, our infrastructure, and our way of life.



(U) Worldwide Cryptologic Platform

- (S//REL) (b)(1) USSC
  (b)(1) USSC
- (U) Multiple Environmental Domains, Multiple Authorities, Complex Policies

(b)(1) USSC

(b)(1) USSC

Graph: (TS/(b)(1))

(b)(1) USSC

Graphic: (TS/(b)(1))

(b)(1) USSC

(TS/(b)(1)/REL) (b)(1) USSC

(b)(1) USSC

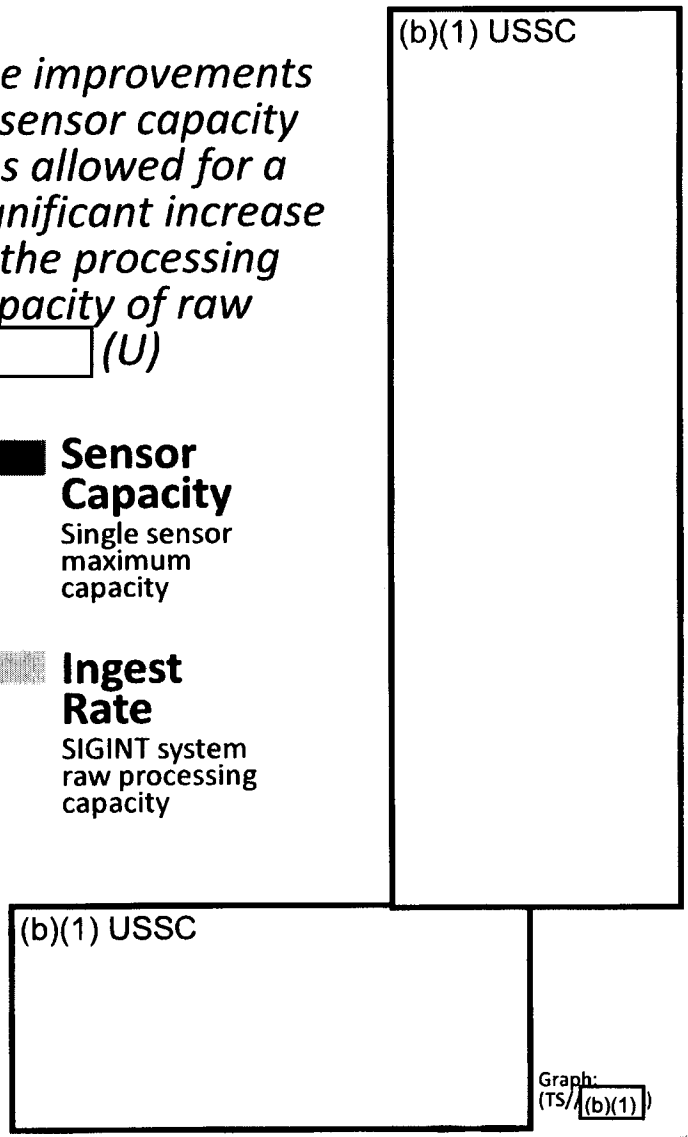
(b)(1) USSC

(U) An Evolving Architecture Leads to Increases in Capability, While Reducing Cost and Power to Process Traffic

The improvements in sensor capacity has allowed for a significant increase in the processing capacity of raw (b)(1) *(U)*

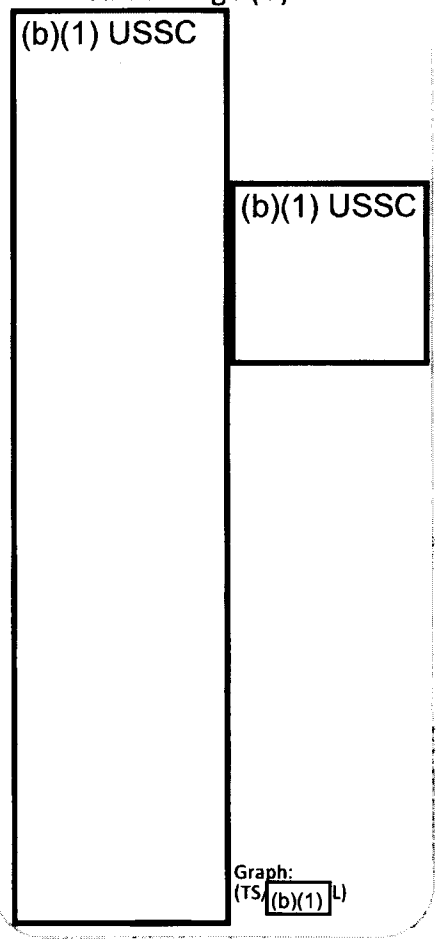
Sensor Capacity
Single sensor maximum capacity

Ingest Rate
SIGINT system raw processing capacity

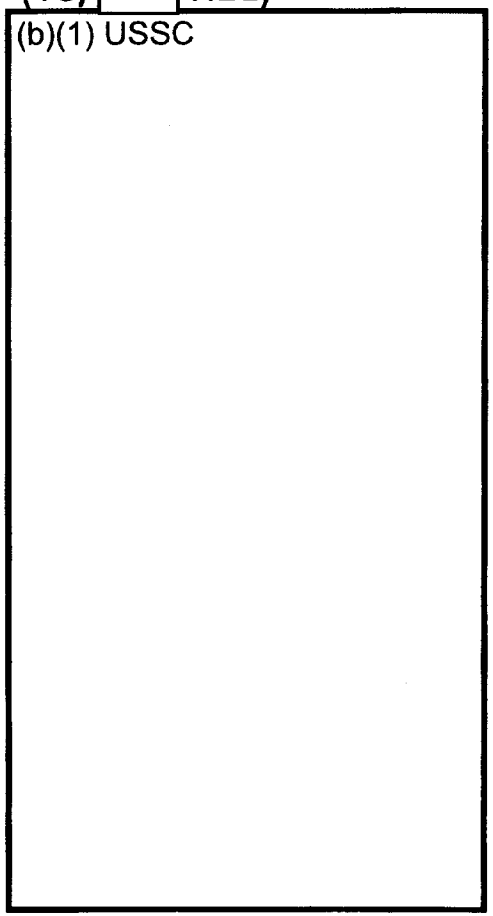


Storage Capacity (U)

(b)(1) system total raw storage (U)

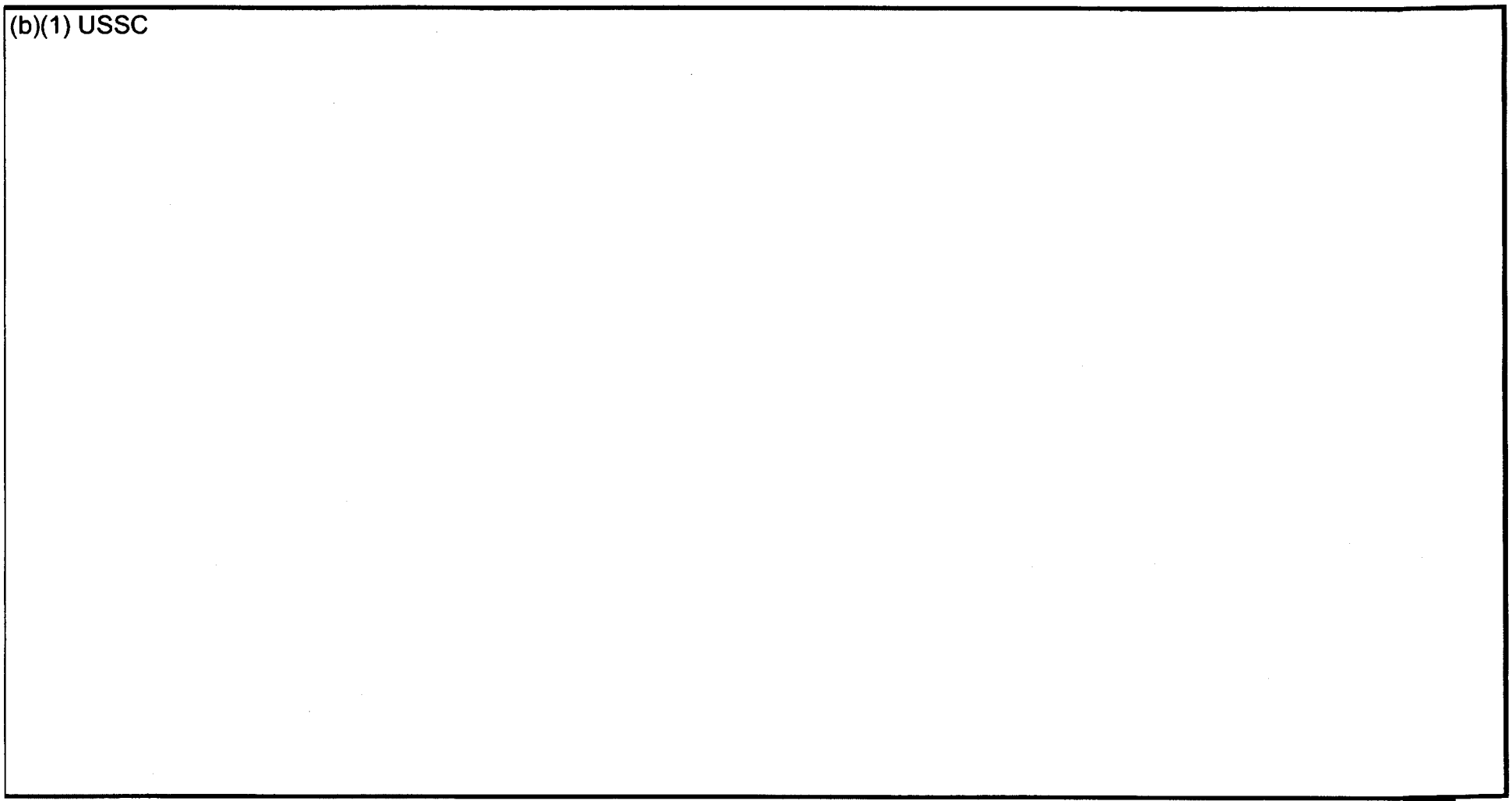


(TS/(b)(1)/REL)



(TS/(b)(1)/NF) (b)(1) USSC

(b)(1) USSC



Graphic: (TS/(b)(1)/)

One day's worth of attack activity (b)(1) USSC

Cyber Threat Briefing

General Keith Alexander

The overall classification of this briefing is: ~~TOPSECRET//~~(b)(1)~~/NOFORN~~

Classified By: cwbean
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380101

U.S. Federal Cybersecurity Operations Team

National Roles and Responsibilities*

US Government Departments and Agencies

DOJ

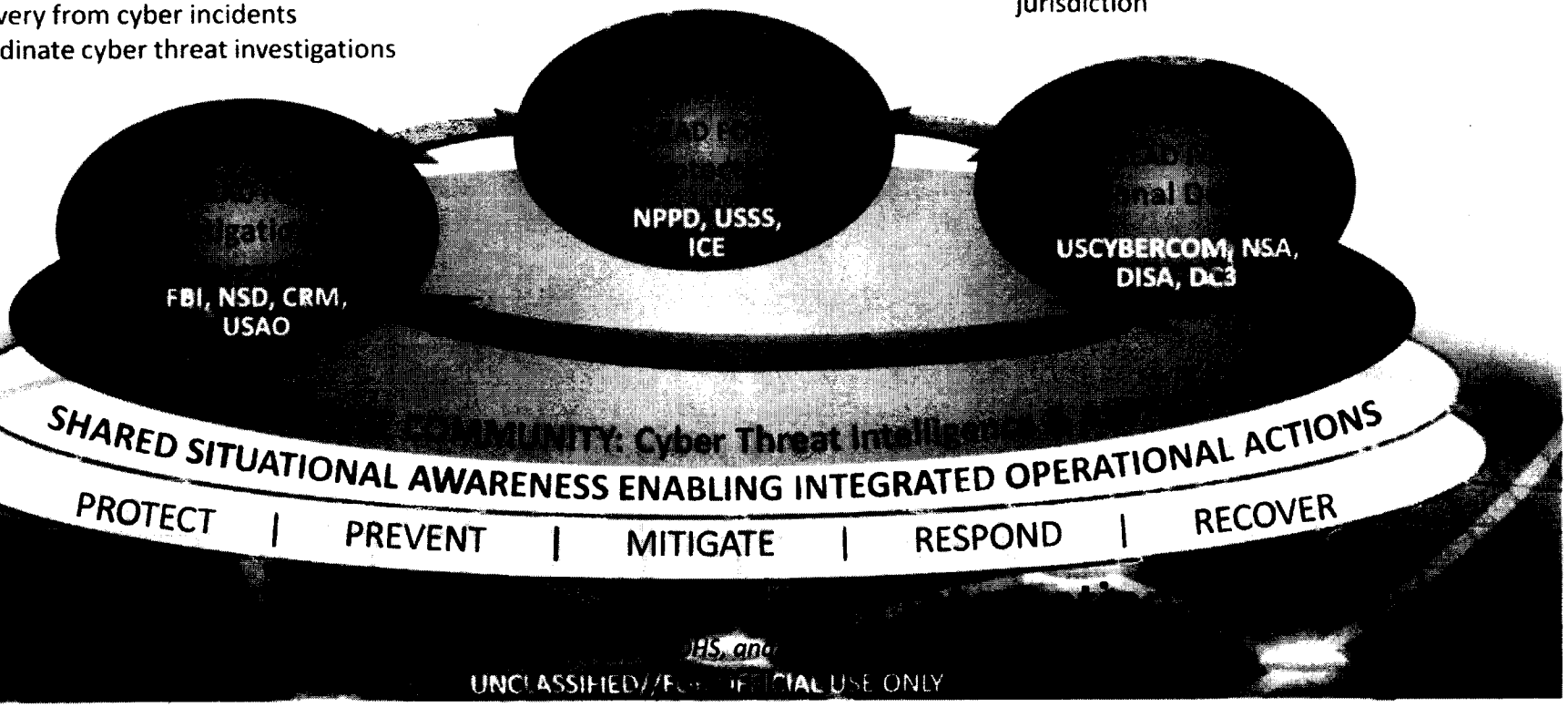
- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

DHS

- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS's jurisdiction

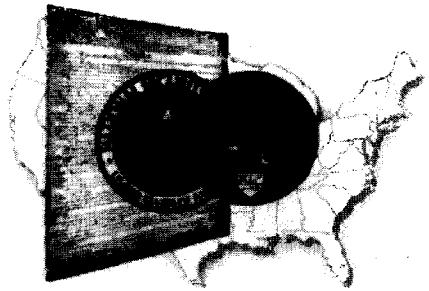
DoD

- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction



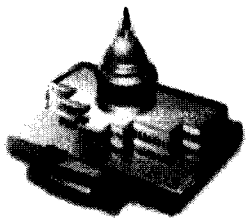
Global Cyberspace

Oversight and Compliance



NSA & USCYBERCOM are committed to protecting privacy and civil liberties.

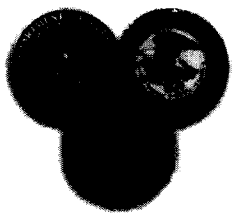
Total Government Approach



Legislative Branch

Key committees:

- Intelligence
- Armed Services
- Judiciary
- Appropriations
- Homeland Security



Executive Branch

- POTUS
- NSA
- DoD
- DNI
- DoJ
- AG

Judicial Branch

- FISA Court: *provides oversight over intelligence activities conducted pursuant to FISA*

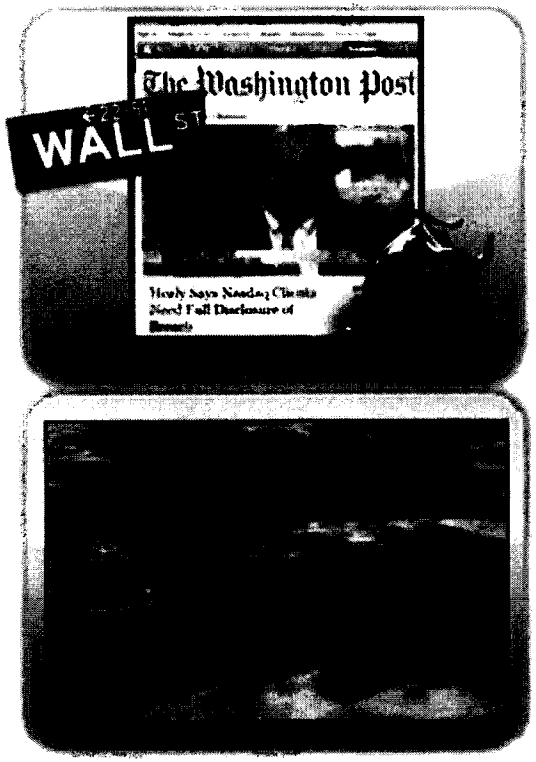
Congressional Role

- Oversight and Compliance
- Authorities: Cyber Legislation, FISA Amendment Act (FAA)
- Mission Oversight
- Resourcing

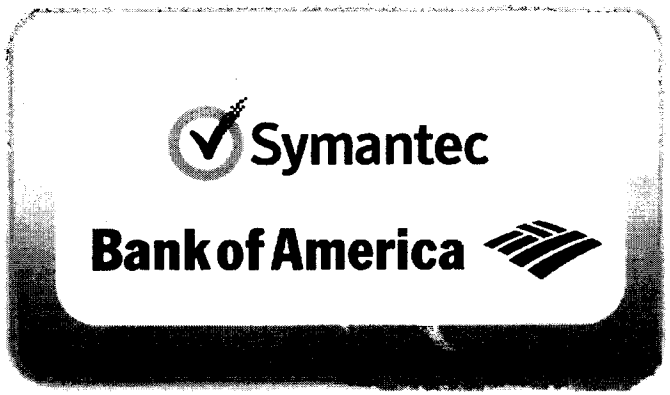
A Disturbing Trend

Exploitation → **Disruption** → **Destruction**

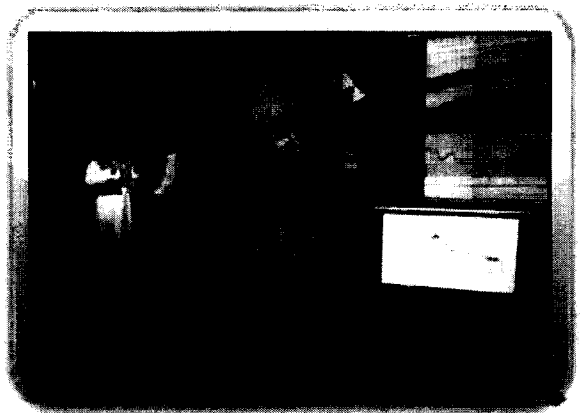
Shady Rat



Denial of Service Attacks



Saudi Aramco



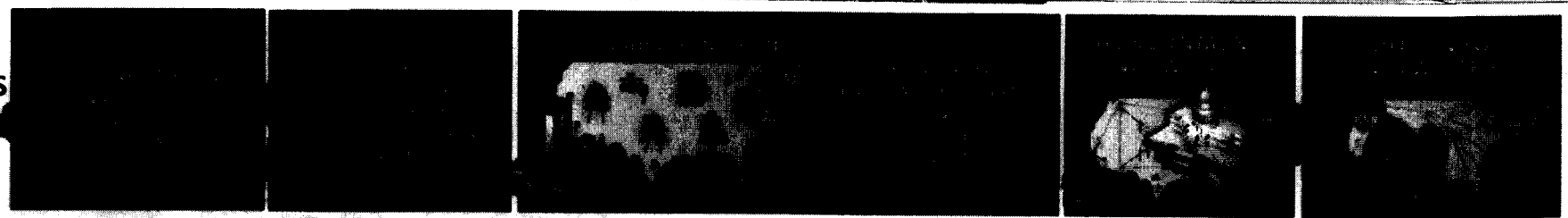
"This is a pre-9/11 moment because the threat is already here…" SecDef Panetta

Overview of Adversary Activity

(b)(1) USSC

state-sponsored

U.S. NETWORKS



CNE, CNA capabilities & unknown activity

Cyber Criminals:
- Botnets
- Spearphishing

(b)(1) USSC

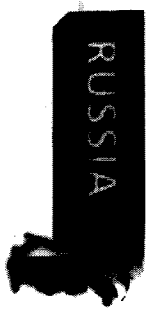
PHOTOS: TS//(b)(1)//L TO USA, FVEY; MAPS & ICONS: U


NAL SECURITY AGENCY
ITED STATES OF AMERICA
RAL SECURITY SERVICE
ITED STATES OF AMERICA

Russia

Russia Cyber Threat

(b)(1) USSC

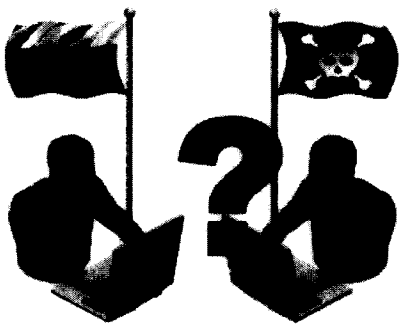


Characteristics

- (b)(1) USSC
-
-

Prevalent Targets

(b)(1) USSC



We surrendered this terrain some time ago…but now we are entering the game again.

Vladimir Putin, 1999

Russian Use of Cyber Attack Tools

RUSSIA

- (b)(1) USSC
-
-
-

The Most Significant Breach of U.S. Military Computers

(b)(1) USSC

RUSSIA

(b)(1) USSC

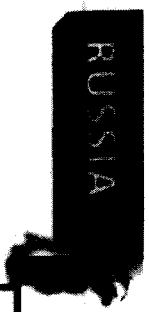
Attribution & Activity Timeline

RUSSIA

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC



First Discovered: (b)(1) USSC

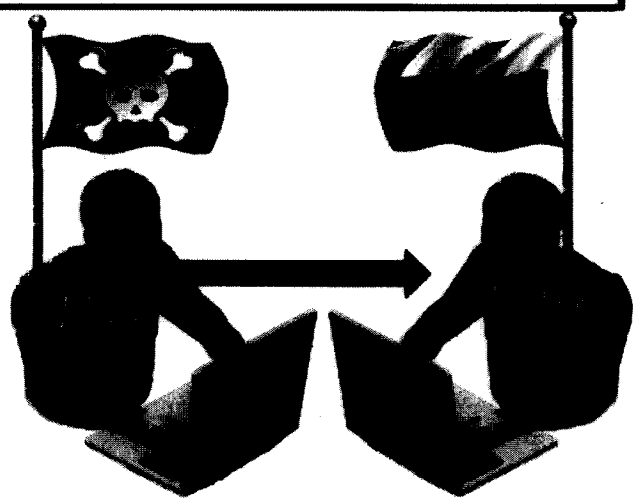
Attribution:

- (b)(1) USSC
-

Targets:

Widespread campaigns against:

- (b)(1) USSC
-
-



Implant Information:

- (b)(1) USSC
-
-
-

(b)(1) USSC

Russian Cybersecurity Threats

(b)(1) USSC

(b)(1) USSC


NAL SECURITY AGENCY
ITED STATES OF AMERICA
EAL SECURITY SERVICE
ITED STATES OF AMERICA

China

China Cyber Threat

(b)(1) USSC

CHINA

Characteristics

- (b)(1) USSC
-
-
-

Prevalent Targets

(b)(1) USSC

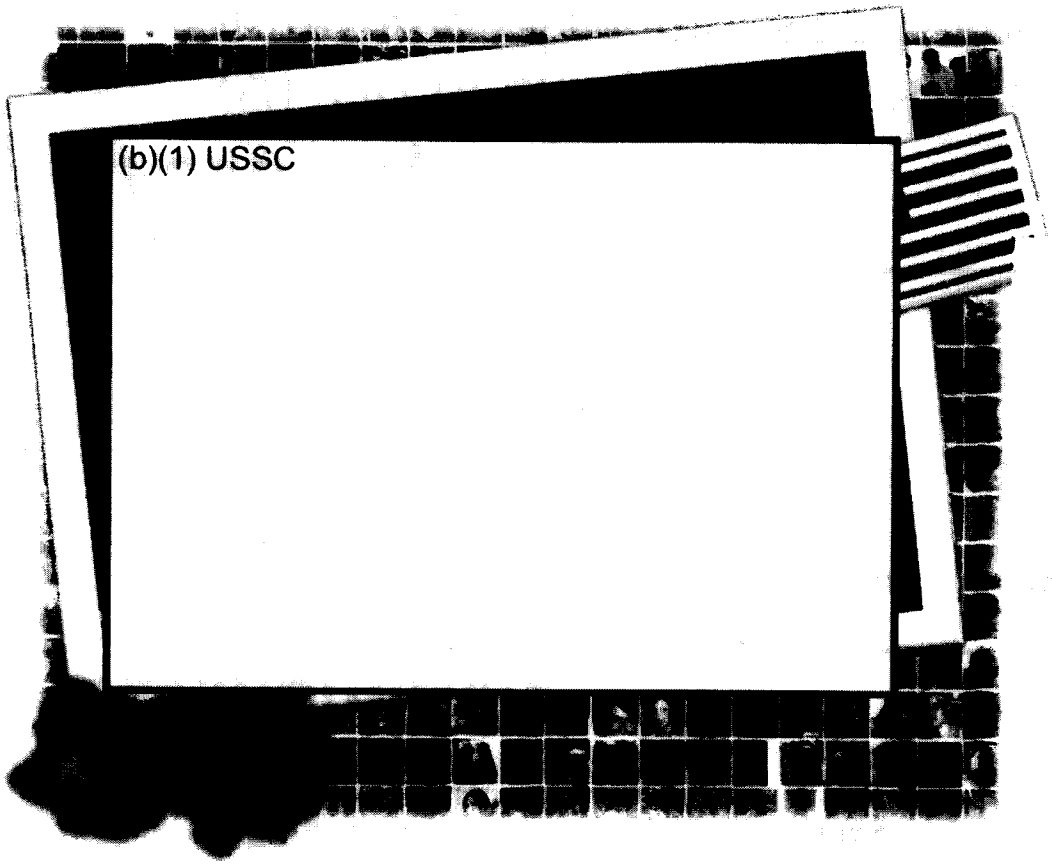
(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

If you are on the internet, the Chinese are probably on your network.

China's Overall Cyber Activity



(b)(1) USSC

(b)(1) USSC

Why is China Doing This Activity?

CHINA

Culturally

(U) It's not perceived as wrong to spy and **steal intellectual property and trade secrets** from adversaries

Economically

(S//NF) (b)(1) USSC

- (b)(1) USSC
-
-
-
-

Politically

(U) Part of **China's national strategy** to have favorable international relations and agreements, and control dissent

China: Cyber Exploitation *and* Attack Units

CHINA

There are a total of

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

Who is Stealing?

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

CHINA

(S//REL TO USA, FVEY) (b)(1) USSC

(b)(1) USSC

How Are They Stealing?

(b)(1) USSC

(b)(1) USSC

(U) **Spear-phishing:** use of a targeted e-mail, possibly nearly indistinguishable from legitimate communications, to lure a victim to open a malicious file or visit a malicious website.

(U) **Vulnerability:** a software or hardware defect or unintended effect.

(U) **Zero-day exploit:** a vulnerability that has not yet been patched or mitigated.

CHINESE INTRUSION SETS

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

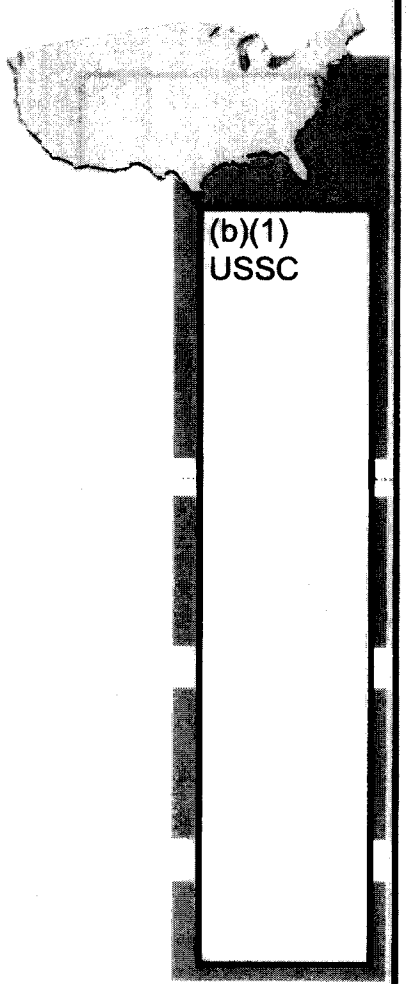
(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

Summary of Intrusion Sets – US Targets



(b)(1) USSC

China:

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

CHINA

(b)(1) USSC

(b)(1) USSC

Chinese Cybersecurity Threats

(b)(1) USSC

(b)(1) USSC

Iran

Cyber: Tool of National Power

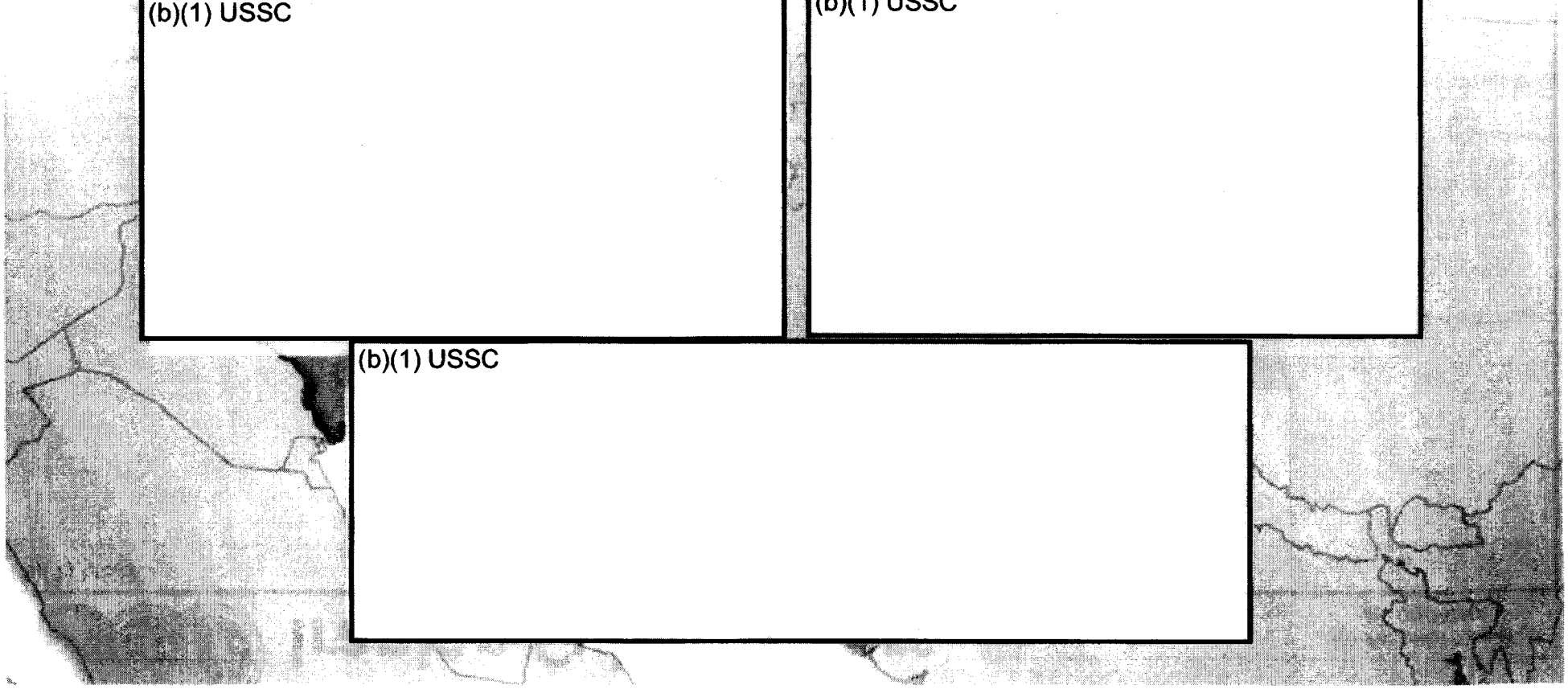
(b)(1) USSC (TS//(b)(1)//NF)

- (b)(1) USSC
-
-

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC



Iranian Cyber Actors

Potential Target for CNO/CNA

(b)(1) USSC

Iranian Cyber Actors (cont.)

(b)(1) USSC

Iranian (b)(1) USSC

IRAN

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

The NSA platform gives us the ability to see in Cyberspace

(b)(1) USSC

The Anatomy of a DDoS Attack

IRAN

(b)(1) USSC

Key Terrain for the Fight
Countering the Adversary

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

IRAN

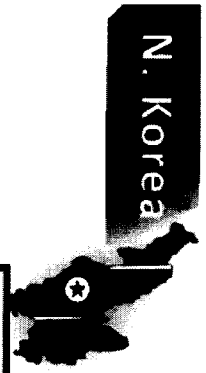
(b)(1) USSC

(b)(1) USSC

Other Actors

North Korea Cyber Threat

(b)(1) USSC

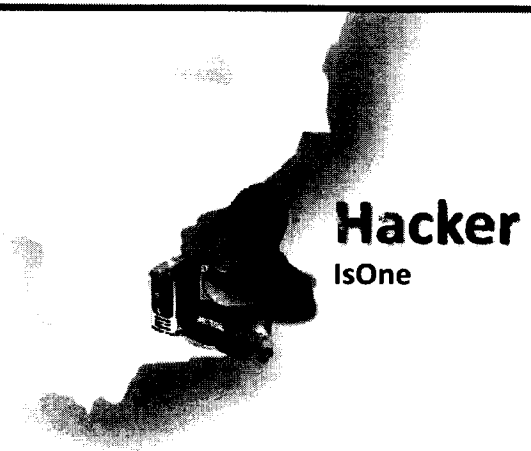


Characteristics

- (b)(1) USSC
-
-
-

Prevalent Targets

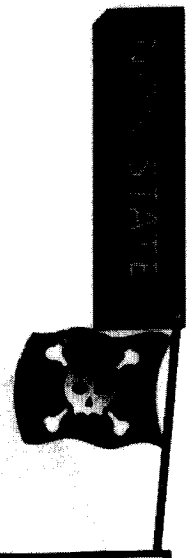
(b)(1) USSC



(b)(1) USSC

Non-State Actors

Worldwide



Characteristics

- (b)(1) USSC

Prevalent Targets

(b)(1) USSC

(b)(1) USSC

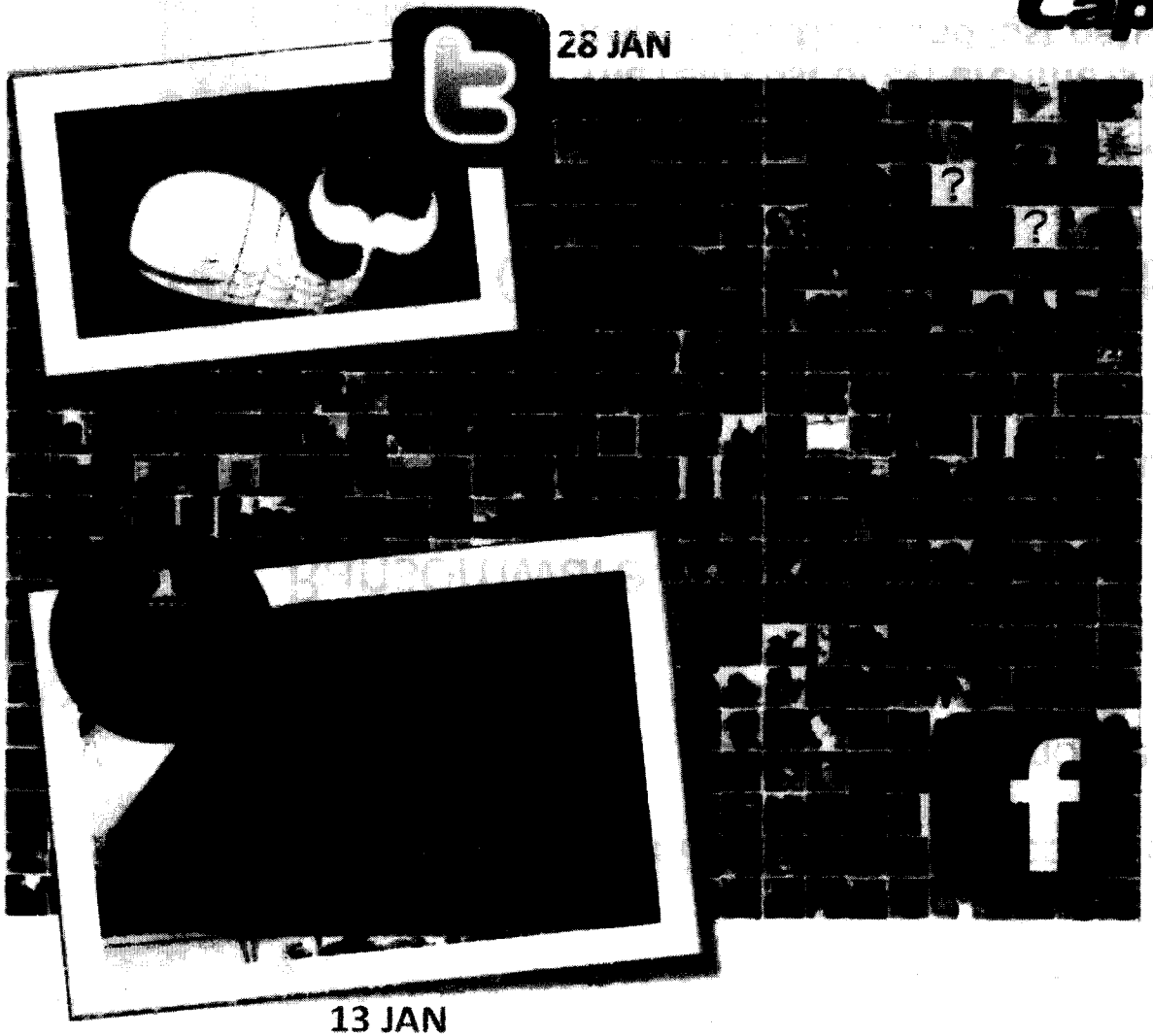
(b)(1) USSC

The future is now

Most recent intrusions

From Open Source:

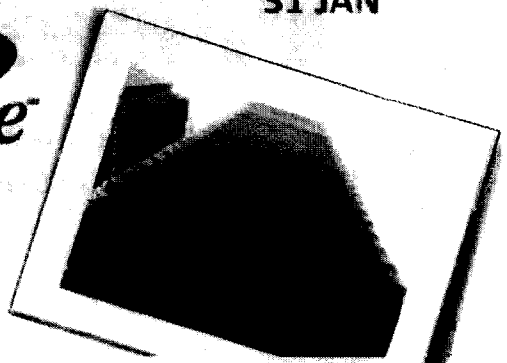
28 JAN



13 JAN

The New York Times

31 JAN



Capital One

24 JAN

THE WALL STREET JOURNAL.

WSJ

1 FEB

From (b)(1) :

(b)(1) USSC

2013 Cyber Predictions Growing & Evolving Threat

Politically motivated attacks will become more destructive *-Trend Micro*

Symantec

As users shift to mobile and cloud, so will attackers *-Symantec*

McAfee SECURE

Ransomware use expands *-Symantec*

Big-scale attacks of more impact to increase *-McAfee*

Rapid evolution and growth in mobile malware *-McAfee*

TREND MICRO

Cyber conflict becomes the norm *-Symantec*

amazon.com

The real cost of cybercrime is in lost business opportunities, lost productivity and lost network operation time.

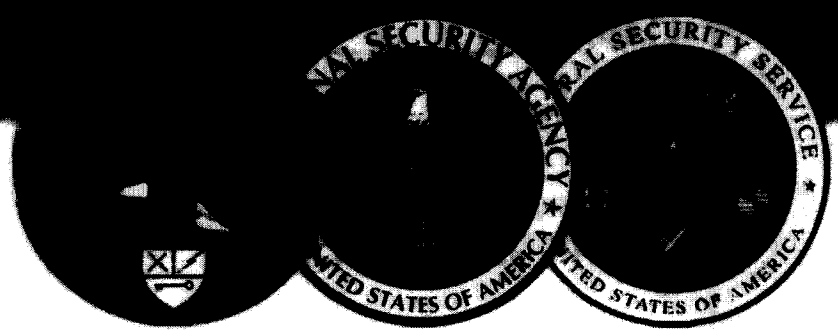
Amazon makes $7 million net profit in an hour. If a DDoS attack takes Amazon.com offline for an hour – Amazon would have lost $7 million dollars and the costs just start there...

Take Aways

- It takes a team to enhance U.S. cybersecurity while protecting civil liberties…and that team is in place
- Congress plays a crucial role
  - Oversight, Resources, Authorities
  - Cybersecurity legislation to protect critical infrastructure
- We are committed to transparency with Congress
  - Work most closely with Intelligence and Armed Services…but are responsive to all members
- We have enjoyed exceptional support and look forward to working with you


NAL SECURITY AGENCY
ITED STATES OF AMERICA
RAL SECURITY SERVICE
ITED STATES OF AMERICA

Questions?


NAVAL SECURITY AGENCY
UNITED STATES OF AMERICA
NAVAL SECURITY SERVICE
UNITED STATES OF AMERICA

Backup

(U) We Cannot Fight If We Cannot See

Logical to Physical (U)
Geolocation of adversary's networks and key nodes, shows relationships between connections in cyber and in physical world

Networks (U)
Enables planning, operations and deconfliction

Geographic Terrain (U)
Critical infrastructure, key actors and key resources

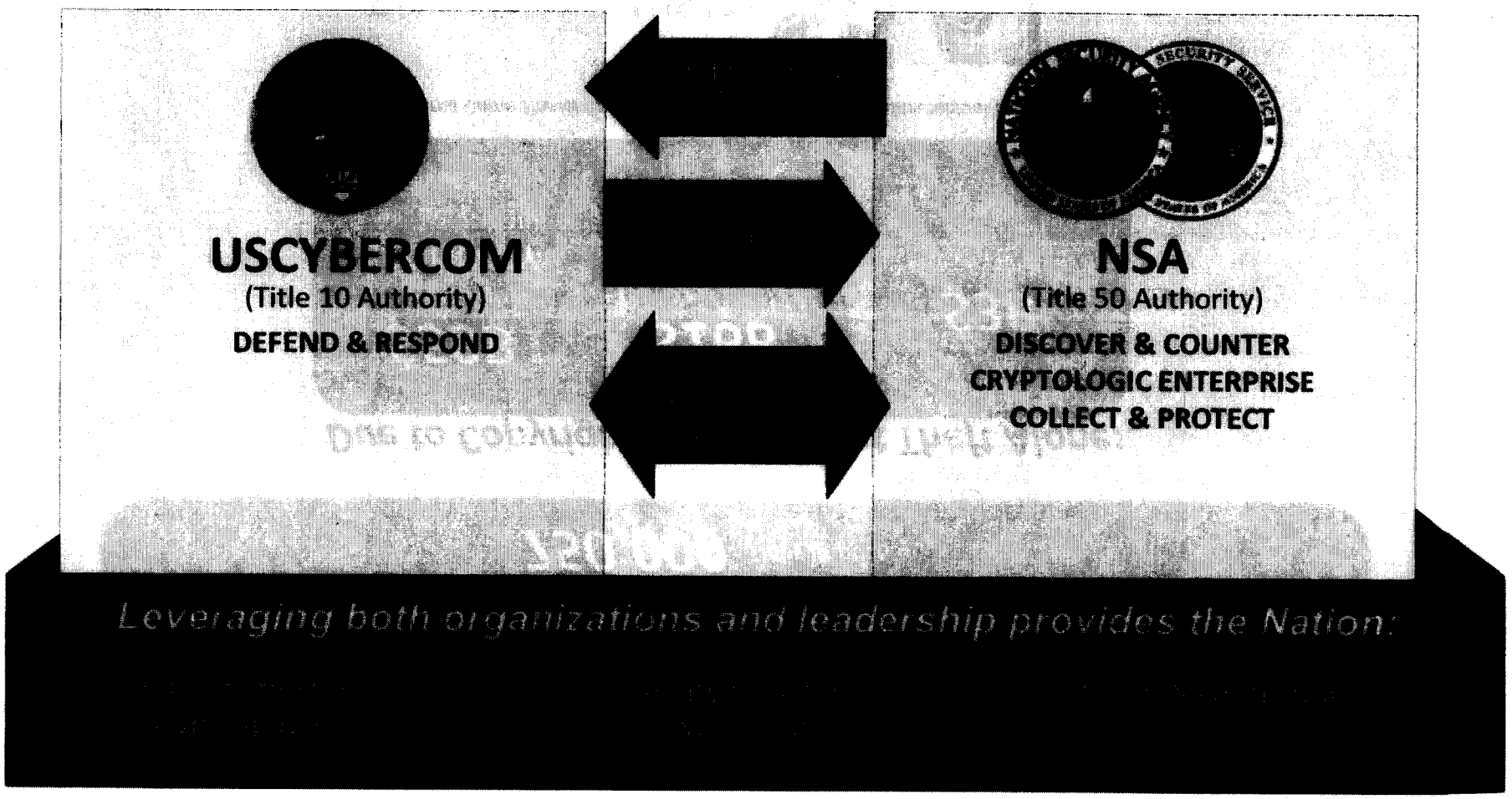
Real-Time Visibility (U)
Networks, adversary attacks, C2 nodes, botnets

(b)(1) USSC **(S//REL)**

(b)(1) USSC

(b)(1) USSC

We Must Fully Leverage the Capabilities of USCYBERCOM & NSA for the Nation



(b)(1) USSC

Impact of Intellectual Property Theft

In 2011, Cost Of IP Theft In The United States Was Estimated At $250B

750,000 *Jobs impacted*

Due to Copyright Infringement Theft Alone:

$58B	$16B	$3B
Lost from the ECONOMY due to copyright infringement	Loss of revenue to COPYRIGHT OWNERS	In tax revenue

Stats from National Crime Prevention Council (www.ncpc.org/topics/intellectual-property-theft)

Estimated value of US IP= **$5.5T**

(TS/ (b)(1) /NF) 2012 Significant Cyber Events

- (b)(1) USSC
-
-
- (b)(1) USSC
- (b)(1) USSC
- (b)(1) USSC
- (b)(1) USSC
- (b)(1) USSC

2013 Predictions – Growing/Evolving Threat

"Politically motivated attacks will become more destructive"

–Trend Micro

Symantec

"Ransomware use expands"

–Symantec

TREND MICRO

"Cyber conflict becomes the norm"

–Symantec

"Rapid evolution and growth in mobile malware"

–McAfee

McAfee SECURE

"Big-scale attacks to increase"

–McAfee

The threat trend is moving toward destructive attacks…

Cyber Legislation

- Incentivize and enable cyber hardening of our critical infrastructure
  - Establish a cyber security standards framework
  - Offer liability protection for cyber intrusion losses to those entities that satisfy the cybersecurity standards

Why we need to get this right:

- We face sophisticated and well resourced state and non-state adversaries
- Core critical infrastructure owners and operators are unable to defend on their own
- Information sharing enables the operational collaboration needed to address threats
- Companies who harden their networks should be afforded liability protection

We can protect civil liberties and secure cyberspace ...