[redacted] (b)(1) [redacted]

The overall classification of this brief is: [redacted] (b)(1) [redacted]

Classified By: alperpe
Derived From: USCYBERCOM SCG
Dated: 20111011
Declassify On: 20371101

UNCLA[redacted] (b)(1) [redacted]

Air Force Incidents

Cyber Threats to USAF Networks

(b)(1) USSC

Cyber Threats to USAF Supply Chain

(b)(1) USSC

Cyber Threats to USAF Platforms

(b)(1) USSC

Key Takeaways

THREAT – (b)(1) USSC

- (b)(1) USSC
-
-

INTENT – (b)(1) USSC

- (b)(1) USSC
-

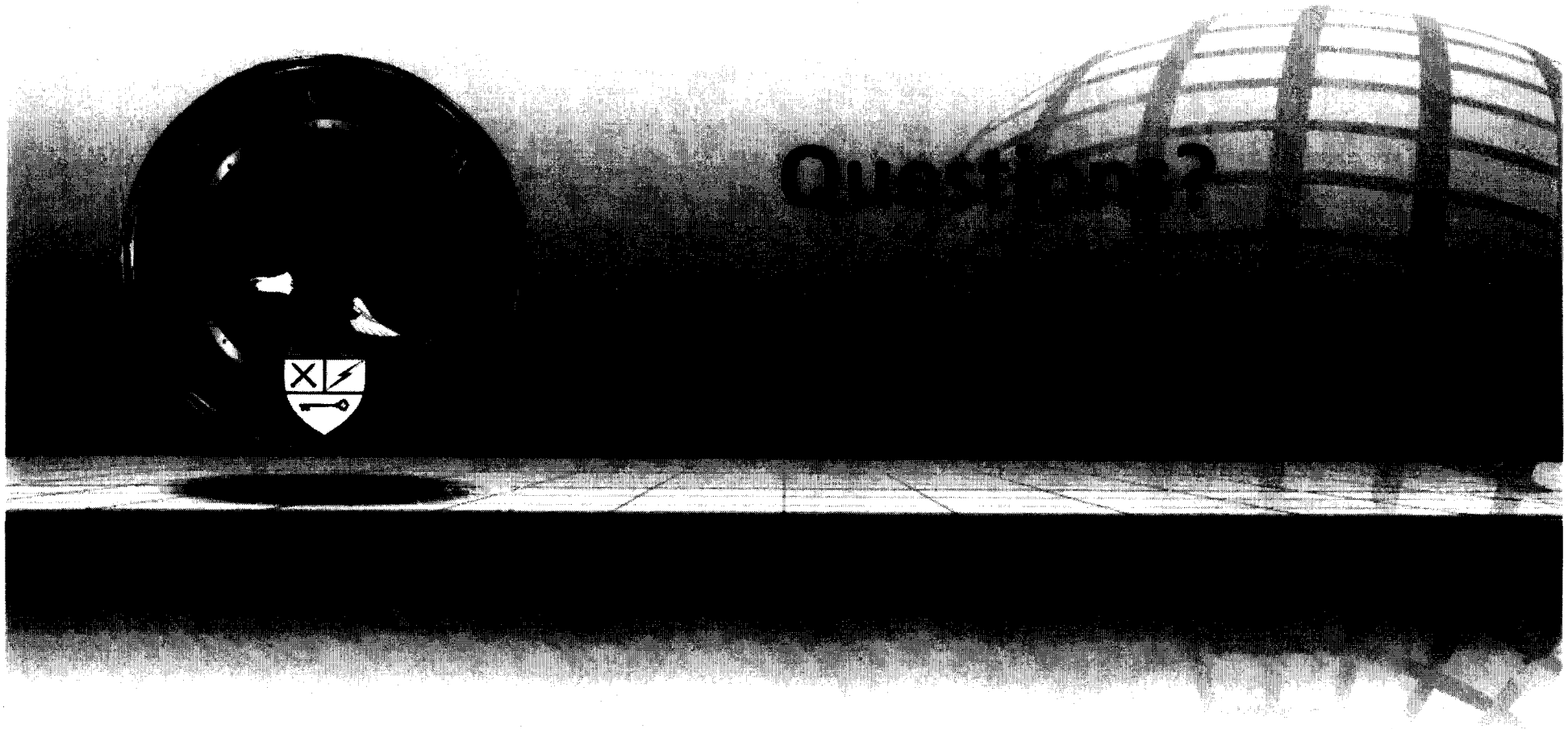
(b)(1) USSC

VULNERABILITY – (b)(1) USSC

- (b)(1) USSC
-

(b)(1) USSC

[redacted] (b)(1) [redacted] USE ONLY



UNCLASS [redacted] (b)(1) [redacted]

SENATE ENGAGEMENT
18 MARCH 2013

TEAM CYBER

- THANK YOU FOR INVITING ME TO HAVE THIS DISCUSSION TODAY.
- AS YOU KNOW, I HAVE THE PLEASURE OF LEADING AN AMAZING TEAM UP AT FORT MEADE BOTH AS THE DIRECTOR OF NSA AND AS THE COMMANDER OF US CYBER COMMAND.

OVERVIEW OF MY DISCUSSIONS

- I'D LIKE TO DISCUSS THE CHALLENGES WE FACE IN PERFORMING THE VITAL MISSION OF KEEPING U.S. MILITARY NETWORKS SECURE, ASSISTING OUR COMBATANT COMMANDERS AROUND THE WORLD, AND WORKING WITH OTHER U.S. GOVERNMENT AGENCIES TO DEFEND OUR NATION AND ITS INTERESTS IN CYBERSPACE.
- I'LL START WITH THE LANES IN THE ROAD WE HAVE FORMULATED WITH DOJ/FBI AND DHS ON HOW WE WORK TOGETHER DEFEND THE NATION BOTH DOMESTICALLY AND ABROAD WHILE PROTECTING CIVIL LIBERTIES AND PRIVACY;
- UPDATE YOU ON THE RECENT CYBER ATTACKS THAT WE HAVE BEEN SEEING FROM IRAN;
- THEN TALK ABOUT BOTH THE ACCESSES WE HAVE AND THE OPERATIONAL PLANNING WE ARE CONDUCTING TO SUPPORT DEFENSE OF THE NATION AND COMBATANT COMMAND PLANNING AND OPERATIONS.

ROLES AND RESPONSIBILITIES (KEY POINTS FROM THE BUBBLE CHART)

- DOD CANNOT DO IT ALONE. NO SINGLE PUBLIC OR PRIVATE ENTITY HAS ALL THE REQUIRED AUTHORITIES, RESOURCES OR CAPABILITIES TO RESPOND TO OR PREVENT A SERIOUS CYBER ATTACK.

~~Classified By: tlphili~~
~~Derived From: USCYBERCOM SCG~~
~~Dated: 20111011~~
~~Declassify On: 20380301~~

- I WORK CLOSELY WITH SECRETARY NAPOLITANO AND DEP SECRETARY LUTE AT DHS, AND WITH DIRECTOR MUELLER AT THE FBI
- WE ALL SEE EYE TO EYE ON THE IMPORTANCE OF SUPPORTING EACH OTHER'S MISSIONS
- FBI – FBI'S ROLE IN DOMESTIC SPACE IS ABSOLUTELY CRITICAL TO DISRUPTING CYBER CRIMINALS AND STOPPING CYBER ATTACKS
    - INVESTIGATE, ATTRIBUTE, DISRUPT AND PROSECUTE CYBER CRIMES.
    - CONDUCT DOMESTIC COLLECTION OF CYBER THREAT INTELLIGENCE
    - THE LEAD FOR INVESTIGATION AND ENFORCEMENT.
- DHS – DHS' WORK TO DEFEND THE .GOV AND TO STRENGTHEN THE SECURITY POSTURE OF CRITICAL INFRASTRUCTURE IS ESSENTIAL; THEY ARE THE LEAD FOR DOMESTIC CYBERSECURITY AND HELP PROTECT FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE
    - COORDINATE THE NATIONAL PROTECTION, PREVENTION, MITIGATION OF, AND RECOVERY FROM CYBER INCIDENTS;
    - LEAD FOR PREVENTION
- DOD/IC –
    - DEFEND THE NATION FROM ATTACK;
    - GATHER FOREIGN CYBER THREAT INTELLIGENCE AND DETERMINE ATTRIBUTION;
    - SUPPORT THE NATIONAL PROTECTION, PREVENTION, MITIGATION OF, AND RECOVERY FROM CYBER INCIDENTS
    - LEAD FOR NATIONAL DEFENSE
- WE CAN'T ACT QUICKLY WITHOUT CLEAR LINES OF RESPONSIBILITY AND RULES OF ENGAGEMENT
- I THINK ALL THREE DEPARTMENTS ARE COMFORTABLE WITH THE ABOVE CONSTRUCT AND THAT IT MAY BE USEFUL TO CONSIDER CODIFYING THOSE RELATIONSHIPS IN ANY LEGISLATION WE ENACT TO MAKE IT CLEAR TO THE PUBLIC THAT THEIR GOVERNMENT IS DEFENDING THE NATIONS BUT WITHIN CONSTITUTIONAL GUIDANCE FOR PROTECTING OUR CIVIL LIBERTIES.

RECENT CYBER ACTIVITIES

- **OVER THE PAST SIX MONTHS, IRANIAN HACKERS HAVE ATTACKED** (b)(1) **FINANCIAL INSTITUTIONS** (b)(1) USSC
- **THE LONGEST ATTACK LASTED OVER** (b)(1) USSC
- (b)(1) USSC
- **THE LATEST SERIES OF ATTACKS BROUGHT DOWN THE** (b)(1) USSC (b)(1) USSC
- **THE IRANIANS CALL THESE ATTACKS** (b)(1) USSC **AND HAVE DESCRIBED** (b)(1) USSC
  - (b)(1) USSC
  -
  -
  - (b)(1) USSC **AMAZON NETS $7MIL PER HOUR IN ONLINE SALES.**
- **SO WHAT DO WE DO ABOUT ANOTHER NATION STATE ATTACKING OUR NETWORKS?**
- **THE TEAM UP AT FORT MEADE IS DOING AS MUCH AS WE ARE AUTHORIZED TO COUNTER THIS ACTIVITY, INCLUDING:**
  1. (b)(1) USSC
  2.
  3. **ALERT THE OTHER CENTERS AT FBI & DHS (NTOC/JOC)**

4. **ALERT THE BANKS (NTOC) (VIA DHS NCCIC)**
5. **DEPLOY INFORMATION ASSURANCE TEAMS TO HELP SHORE UP NETWORKS WHEN REQUESTED TO DO SO (NSA IAD AND USCYBERCOM).**
6. (b)(1) USSC
7.

- (b)(1) USSC
-

- **EXECUTION OPTIONS:**
  - (b)(1) USSC
  -
  -

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

- **KEY TAKEAWAY: (b)(1) USSC IS THE RADAR THAT ALLOWS USCYBERCOM TO SEE THE ADVERSARY IN THIS DOMAIN.**
- **YOU CAN'T FIGHT WHAT YOU CAN'T SEE AND NSA HAS THE BEST PICTURE OF THE KEY TERRAIN FOR THIS FIGHT.**

- **<u>SAUDI ARAMCO</u>**
- **IN AUGUST, SAUDI ARAMCO WAS HIT WITH A DESTRUCTIVE ATTACK THAT DESTROYED THE DATA ON MORE THAN 30,000 SYSTEMS, (b)(1) USSC**
  - (b)(1) USSC
    - (b)(1) USSC
  - (b)(1) USSC
    - (b)(1) USSC
- **WHAT KEEPS ME UP AT NIGHT IS KNOWING THAT ANOTHER NATION THAT HAS DEMONSTRATED CAPABILITY FOR DESTRUCTIVE NETWORK ATTACK IS CURRENTLY CONDUCTING DISRUPTIVE ATTACKS AGAINST OUR FINANCIAL NETWORKS.**
- (b)(1) USSC

(b)(1) USSC

- (b)(1) USSC
  - (b)(1) USSC
- (b)(1) USSC
  - (b)(1) USSC
  -
  -
  -
  -
- (b)(1) USSC
  - (b)(1) USSC
  -
- **CCMTS: AS FAR AS CYBER COMBAT MISSION TEAMS (CCMTS), IT IS IMPORTANT TO NOTE THAT CCMTS SUPPORT COMBATANT COMMAND (CCMD) MISSIONS AND, CONSEQUENTLY THESE TEAMS' FOCUS AREAS WILL BE DEVELOPED BASED ON CCMD PRIORITIES.**
- (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
  - (b)(1) USSC
  -
- (b)(1) USSC

- (b)(1) USSC

OUR OFFENSIVE AND DEFENSIVE TEAMS WORK TOGETHER

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

- (b)(1) USSC
-

- (b)(1) USSC
- (b)(1) USSC **DOD DECIDED TO REALIGN JTF-GNO UNDER JFCC-NW AND SUBSEQUENTLY INCLUDED AS A PART OF THE STAND UP OF USCYBERCOM.**
- **THE SUCCESS OF DOD'S ABILITY TO FIGHT AND WIN IN CYBERSPACE IS INEXTRICABLY LINKED TO THE NATION'S WORLD CLASS CRYPTOLOGIC PLATFORM.**

~~TOP SECRET/~~ (b)(1) ~~NOFORN~~

HOUSE APPROPRIATIONS COMMITTEE-DEFENSE (HAC-D) HEARING
6 MARCH 2013

OPENING COMMENTS

- THANK YOU VERY MUCH CHAIRMAN YOUNG AND RANKING MEMBER VISCLOSKY FOR INVITING ME TO SPEAK TODAY ON BEHALF OF THE MEN AND WOMEN OF U.S. CYBER COMMAND AND THE NATIONAL SECURITY AGENCY
- I HAVE THE HONOR OF LEADING THESE MEN AND WOMEN ON A DAILY BASIS. THERE IS NO FINER AND MORE DEDICATED TEAM OF SERVICE MEMBERS AND CIVILIAN PERSONNEL ANYWHERE.
- I'D LIKE TO SPEAK TODAY ABOUT THE CHALLENGES WE FACE IN PERFORMING THE VITAL MISSION OF KEEPING U.S. MILITARY NETWORKS SECURE, ASSISTING OUR COMBATANT COMMANDERS AROUND THE WORLD, AND WORKING WITH OTHER U.S.

~~Classified By: jarob11~~
~~Derived From: USCYBERCOM SCG~~
~~Dated: 20111011~~
~~Declassify On: 20380201~~

~~TOP SECRET/~~ (b)(1) ~~NOFORN~~

GOVERNMENT AGENCIES TO DEFEND OUR NATION AND ITS INTERESTS IN CYBERSPACE.

- SINCE LAST YEAR, EVENTS IN CYBERSPACE HAVE EVOLVED RAPIDLY
- THREATS IN CYBERSPACE CONTINUE TO ADVANCE AND GROW
- WE ARE WORKING TO SECURE OUR NETWORKS BUT THERE IS MUCH MORE TO DO TO PROTECT OURSELVES FROM THESE THREATS

(U/~~/FOUO)~~ ROLE OF DOD:

- I'LL ADDRESS SOME OF THESE THREATS IN A FEW MOMENTS
- BUT FIRST I WANT TO FRAME OUR DISCUSSION WITH A FEW POINTS ON THE ROLE OF THE DOD AND THE IMPERATIVE THAT WE OPERATE IN CYBERSPACE WITH UNCOMPROMISING CONCERN FOR PROTECTING CIVIL LIBERTIES AND COMPLYING WITH THE CONSTITUTION AND LAWS OF OUR NATION
- THREE MAIN FUNCTIONS:
    - DEFEND THE NATION FROM ATTACK IN CYBERSPACE
    - SUPPORT COCOM PLANNING AND OPS

- OPERATE AND SUSTAIN DOD INFORMATION NETWORKS

- WE MUST ALSO GATHER CYBER THREAT INTELLIGENCE, AND SUPPORT THE NATIONAL PROTECTION, PREVENTION, MITIGATION OF, AND RECOVERY FROM CYBER INCIDENTS

(U//~~FOUO~~) BUBBLE CHART

- BUT DOD CANNOT DO IT ALONE. NO SINGLE PUBLIC OR PRIVATE ENTITY HAS ALL THE REQUIRED AUTHORITIES, RESOURCES OR CAPABILITIES TO RESPOND TO OR PREVENT A SERIOUS CYBER ATTACK.
- I WORK CLOSELY WITH SECRETARY NAPOLITANO AND DEP SECRETARY LUTE AT DHS, AND WITH DIRECTOR MUELLER AT THE FBI
- WE ALL SEE EYE TO EYE ON THE IMPORTANCE OF SUPPORTING EACH OTHER'S MISSIONS
  - FBI'S ROLE IN DOMESTIC SPACE IS ABSOLUTELY CRITICAL TO DISRUPTING CYBER CRIMINALS AND STOPPING CYBER ATTACKS
  - LIKEWISE, DHS' WORK TO DEFEND THE .GOV AND TO STRENGTHEN THE SECURITY POSTURE OF CRITICAL INFRASTRUCTURE IS ESSENTIAL; THEY ARE THE LEAD FOR

DOMESTIC CYBERSECURITY AND HELP PROTECT FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

- WE CAN'T ACT QUICKLY WITHOUT CLEAR LINES OF RESPONSIBILITY AND RULES OF ENGAGEMENT

(U//~~FOUO~~) CIVIL LIBERTIES AND OVERSIGHT & COMPLIANCE

- THE ISSUANCE OF THE EO LAST MONTH WAS A GREAT STARTING POINT TO PROTECTING OUR NETWORKS AND OUR INTELLECTUAL PROPERTY
- NSA AND CYBERCOM REMAIN COMMITTED TO DEFENDING OUR NATION IN CYBERSPACE AND PROTECTING OUR CRITICAL INFRASTRUCTURE
- AND WE ARE COMMITTED TO SUPPORTING THE RIGHTS ENSHRINED IN THE CONSTITUTION, TO INCLUDE THE RIGHT TO PRIVACY & CIVIL LIBERTIES
- WE CAN CONDUCT BOTH OF THESE MISSIONS, DEFEND THE NATION & ENSURING PRIVACY/CIVIL LIBERTIES, SIMULTANEOUSLY
- WE TAKE A TOTAL GOVERNMENT APPROACH TO PROTECTING THESE RIGHTS; THROUGH

CONGRESS, THE EXECUTIVE BRANCH AND THE JUDICIAL BRANCH

- CONGRESS PLAYS A CRITICAL ROLE BY PROVIDING OVERSIGHT, GRANTING AUTHORITIES, AND ALLOCATING RESOURCES
- WE CAN PROTECT OUR NATION WHILE ADDRESSING GROWING THREATS

(U) DISTURBING TREND

- CERTAIN NATION STATES HAVE RESOURCED NATIONAL STRATEGY TO GROW ECONOMY BY EXPLOITING R&D FROM LEADING TECH COMPANIES ACROSS THE GLOBE
- TARGET LARGE & SMALL U.S. COMPANIES
- DESTRUCTIVE ATTACKS ON THE RISE
  - AUGUST 2012 – SHAMOON INFECTED MORE THAN 30,000 COMPUTERS IN SAUDI ARABIA'S ARAMCO
  - SIMILAR ATTACK ON RASGAS OF QATAR
- HERE IN THE US, INTRUSIONS OCCURRING AGAINST BEST IN THE SECURITY BUSINESS.
  - 2012: SYMANTEC, MASTER CARD, VISA
  - OVER THE PAST 6 MONTHS, MULTIPLE ATTACKS AGAINST WALL STREET & US BANKS

- **IT IS NOT GOING TO GET ANY BETTER; INDICATIONS OF WHAT'S TO COME**

(U) OVERVIEW OF ADVERSARY ACTIVITY

- **CHARACTERIZING THE THREAT FROM CHINA, IRAN AND RUSSIA**
  - **(TS** (b)(1) **REL)** (b)(1) USSC
    (b)(1) USSC
  - **(TS** (b)(1) **REL)** (b)(1) USSC
    (b)(1) USSC
  - **(TS** (b)(1) **REL)** (b)(1) USSC
    (b)(1) USSC
- **LET ME FOCUS ON RUSSIA FIRST**

(U) RUSSIA THREAT

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

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

(U) CHINA CYBER THREAT

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

  - (b)(1) USSC
  -

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

(b)(1) USSC

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

(b)(1) USSC

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

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

(b)(1) USSC

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

(s) ~~(U)~~ (b)(1)

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

(U) CHINA: FOR-PROFIT CNE

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

(U) 4PLA

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

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

(U) ASSESSMENT OF CHINESE ACTIVITY

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

(U) IRAN CYBER THREAT

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

(b)(1) USSC

- (TS (b)(1) NF) (b)(1) USSC

(b)(1) USSC

- (b)(1) USSC
-
-

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

(b)(1) USSC

- (b)(1) USSC
-
-

- (TS (b)(1) NF) (b)(1) USSC

(b)(1) USSC

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

(U) NORTH KOREA CYBER THREAT

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

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

(b)(1) USSC

(U) CYBER THREAT FROM NON-STATE ACTORS

- **CYBER CRIME IS THRIVING ECOSYSTEM WHICH SOME ESTIMATE IS RESPONSIBLE FOR FINANCIAL LOSS WORLDWIDE IN THE HUNDREDS OF BILLIONS OF DOLLARS**

- **NON STATE AND NON TRADITIONAL ACTORS VERY ACTIVE; LEVERAGE TRANSNATIONAL SKILLS**
- **CRIMINAL FORUMS INCREASE EVERY MONTH ALONG WITH INCREASE IN MALWARE**
- **MOTIVATED BY PROFIT**

(U) INTRUSIONS

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

(b)(1) USSC

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

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

(b)(1) USSC

- (b)(1) USSC
-
-
-

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

(U) 2013 CYBER PREDICTIONS

- **ATTACKS MORE DESTRUCTIVE**
- **RAPID EVOLUTION OF GROWTH IN MOBILE MALWARE**
- **CONTINUED EXPLOITATION OF US IP**

(U) 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**
- **WE ARE COMMITTED TO TRANSPARENCY**

Russia Cyber Threat

[redacted]

(b)(1) USSC

Actors / Groups

[redacted]

US Sectors targeted

[redacted] (b)(1) USSC

Leadership awareness

[redacted]

China Cyber Threat

Characterization	(b)(1) USSC
Actors / Groups	
Primary Targets	
US Sectors targeted	
Stats from (b)(1) USSC	
Leadership awareness	
Trends / forv	

Iran Cyber Threat

(b)(1) USSC

Actors / Groups

US Sectors targeted

(b)(1) USSC

Leadership awareness

[redacted] (b)(1)

Cyberspace Operations

General Keith Alexander, USA
Commander, USCYBERCOM
Director, National Security Agency
Chief, Central Security Services

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

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

U.S. Federal Cybersecurity Operations Team

National Roles and Responsibilities*

DOJ

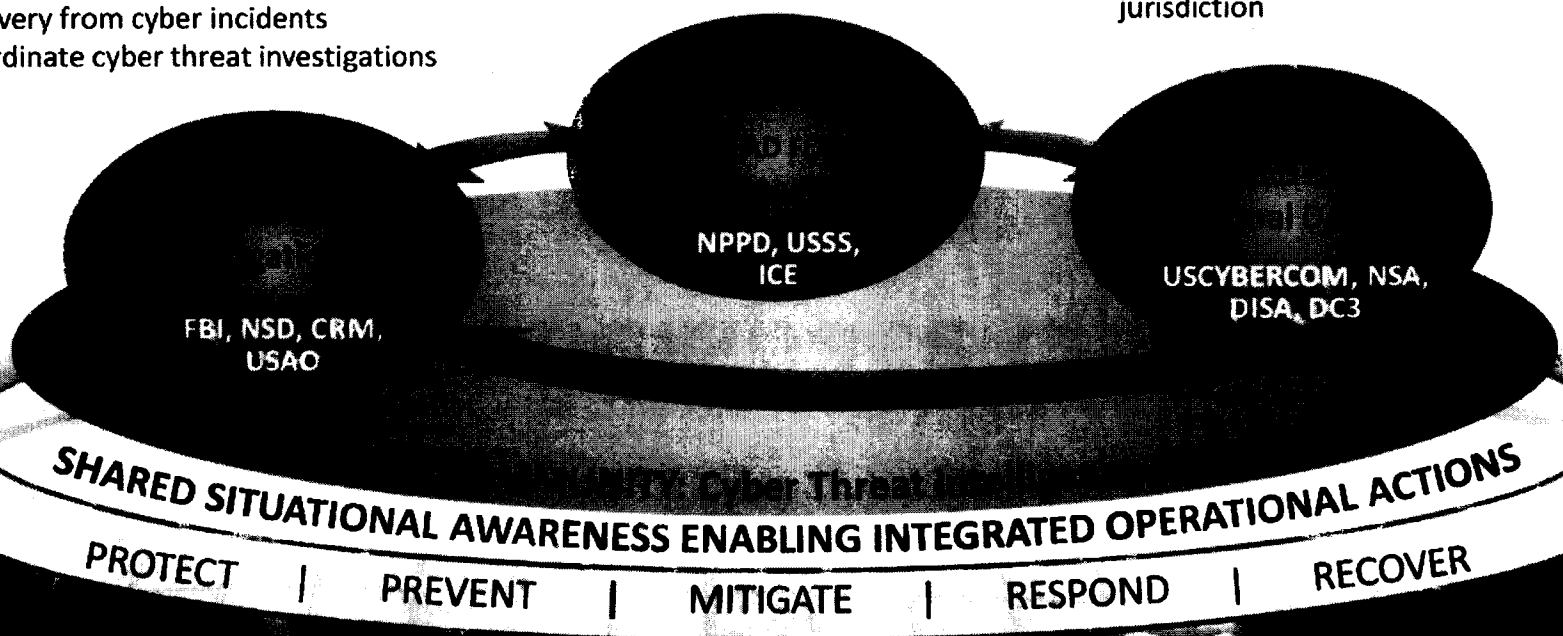
- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate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



TAO Slides placeholder

One-day DDoS snap-shot

(b)(1) USSC

DDoS event vs (b)(1) USSC

(b)(1) USSC

The Anatomy of a DDoS Attack

(b)(1) USSC

How We Operate Globally to Defend the U.S.

(b)(1) USSC

(b)(1) USSC

How Cyber Supports the Combatant Commander

Action Against the Adversary

(b)(1) USSC

MAP: TS/[redacted] (b)(1) TO USA, FVEY

Team Cyber Updates

(b)(1) USSC

(b)(1) USSC

Team Cyber Updates

(b)(1) USSC

Team Cyber Updates

(b)(1) USSC

We Must Synchronize & Deconflict Operations

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

Cyber Mission Forces

(b)(1) USSC

(b)(1) USSC

(b)(1)

Questions?

(b)(1) USSC

(b)(1) USSC

(b)(1)

(b)(1) USSC

(b)(1)

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

Response Options for the National Mission Fight

Countering the Adversary

(b)(1) USSC

(b)(1)

U.S. Federal Cybersecurity Operations Team

National Roles and Responsibilities

DOJ

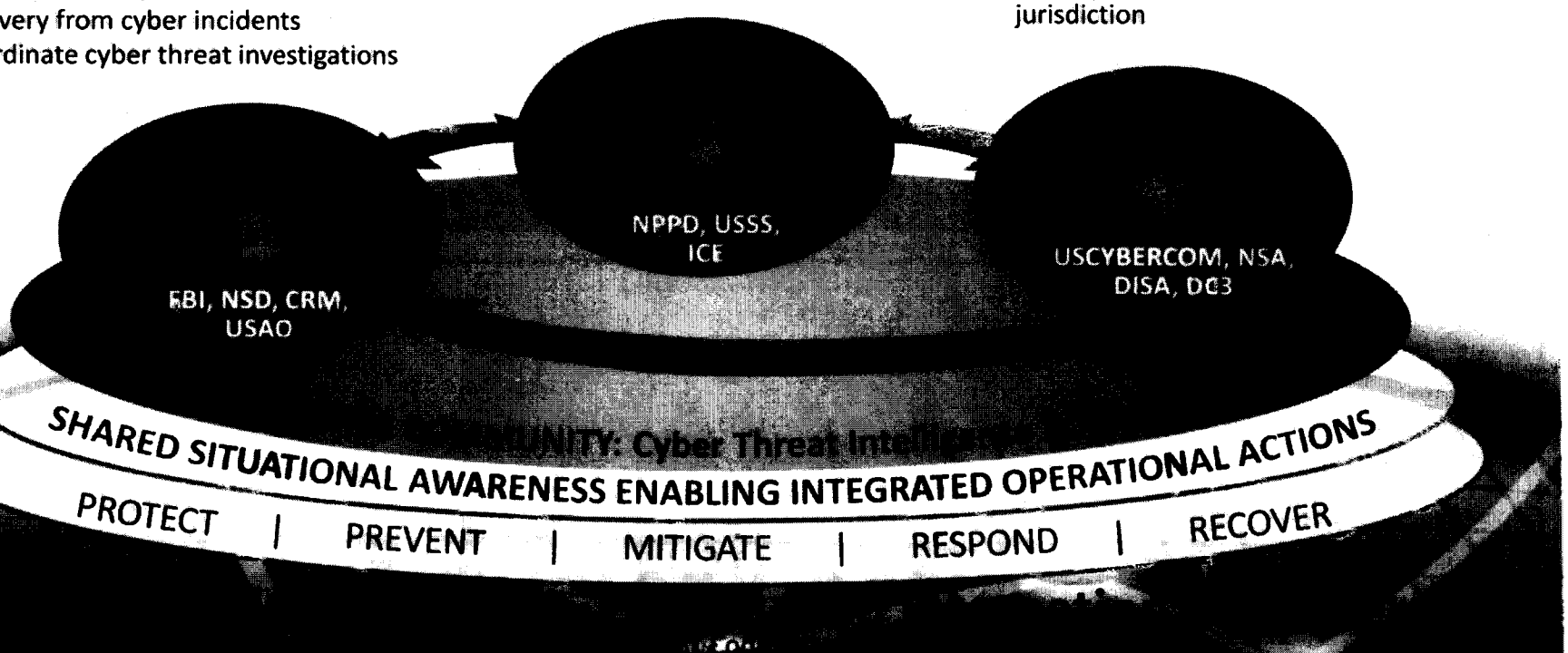
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

DHS

- Coordinate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS's jurisdiction

DoD

- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction



(b)(1)

State-sponsored Threats

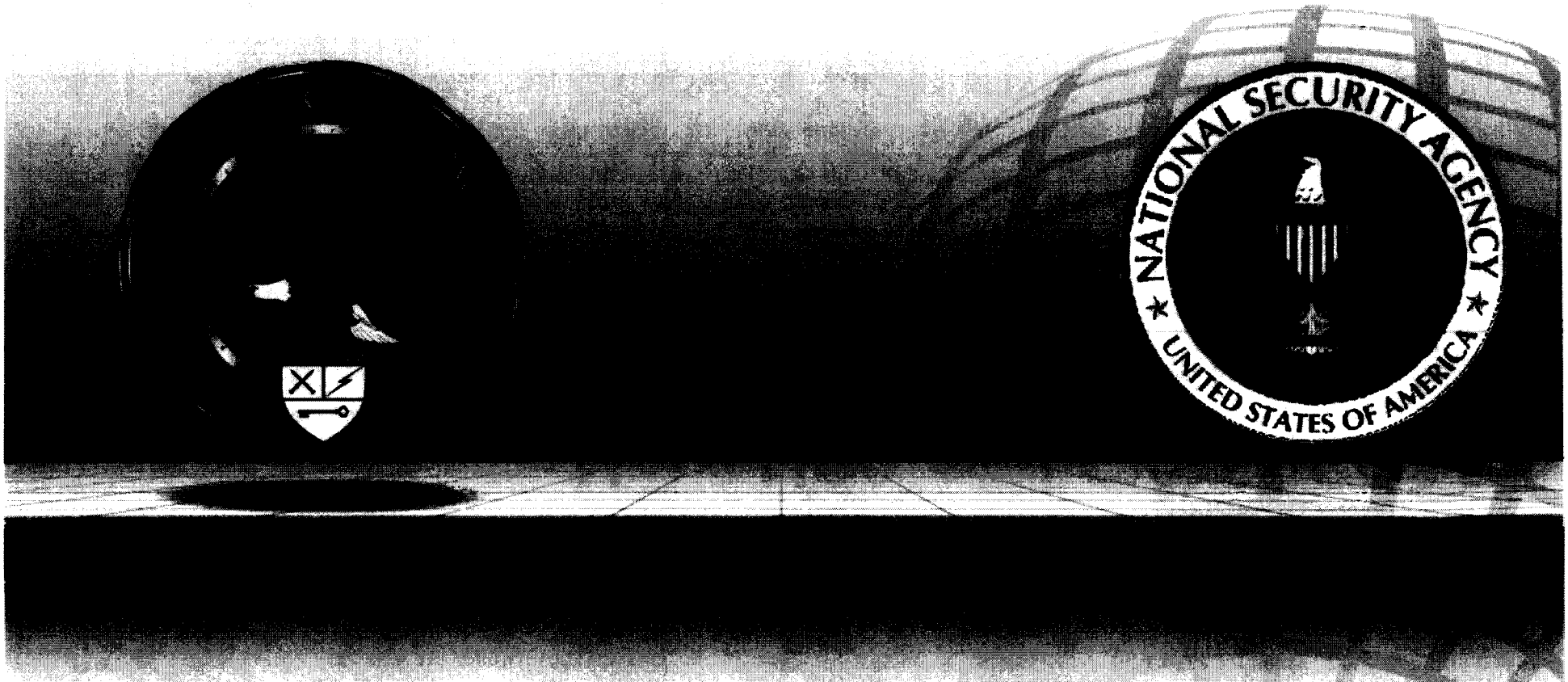
(b)(1) USSC

U.S. NETWORKS

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

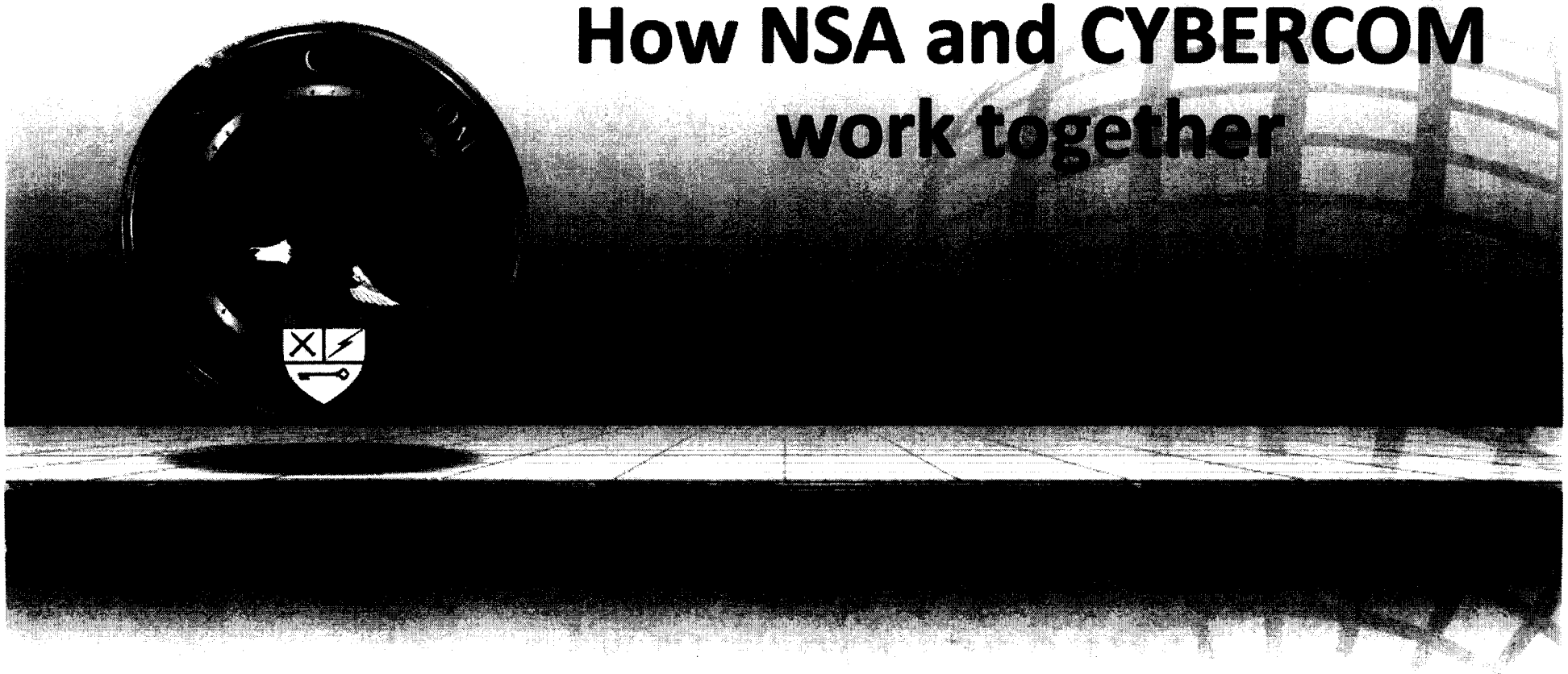
(b)(1) USSC

Cyberspace Security
Mr. Daniel



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

A Cyber Story: How NSA and CYBERCOM work together



HOW (b)(1) AND CYBER WORK TOGETHER

THE STORY BEGINS

HOW (b)(1) AND CYBER WORK TOGETHER

(b)(1) USSC

U.S. Decision Makers

INFORMATION

(b)(3) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

HOW (b)(1) AND CYBER WORK TOGETHER

(b)(1) USSC

INFORMATION
OPTIONS

(b)(3) USSC

(b)(1) USSC

(b)(1) USSC

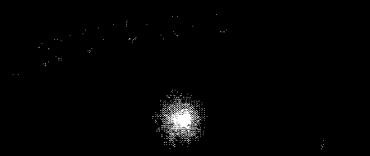
(b)(1) USSC

HOW (b)(1) AND CYBER WORK TOGETHER

(b)(1) USSC

U.S. Decision Makers

INFORMATION
OPTIONS
SOLUTIONS



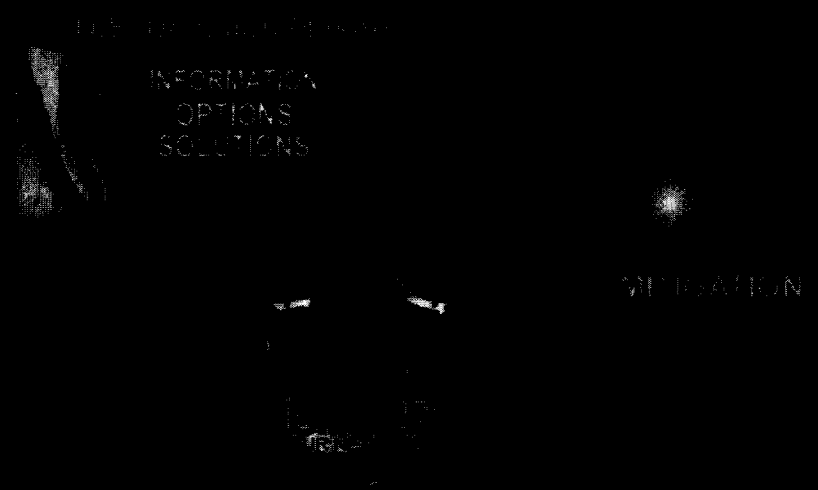
MITIGATION

(b)(3) USSC

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

HOW (b)(1) AND CYBER WORK TOGETHER

(b)(1) USSC



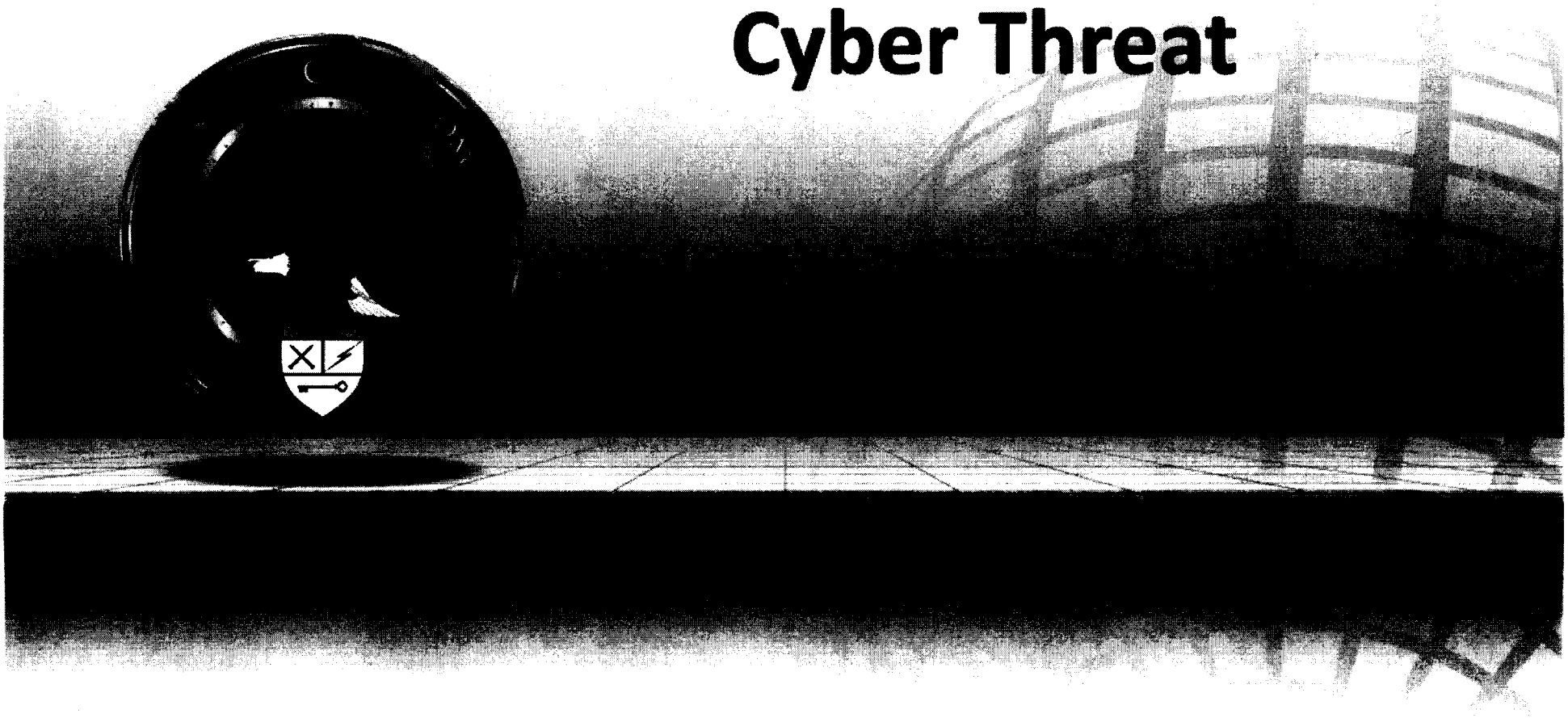
(b)(3) USSC

(b)(1) USSC

(b)(1) USSC

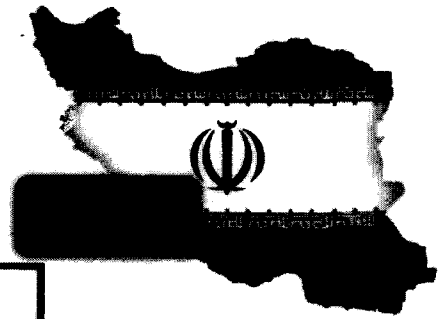
(b)(1) USSC

Cyber Threat



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

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



Graphic is UNCLASSIFIED

(U) STRATEGY

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

(U) CAPABILITIES

- (U)Forces:
  - IRGC-QF (U)
  - Associated Terrorist Organizations (U)
  - (b)(1) USSC (b)(1) USSC (TS/(b)(1)/NF)
- (U)Tools / TTPs:
  - DDoS ~~(TS/(b)(1)/NF)~~
  - Insider Recruitment ~~(TS/(b)(1)/NF)~~
  - Spearphishing ~~(TS/(b)(1)/NF)~~
  - Custom built malware / Cybercrime developed malware ~~(TS/(b)(1)/NF)~~

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

- (b)(1) USSC

2007

- (b)(1) USSC

EARLY-2008

- (b)(1) USSC

MID-2008

- (b)(1) USSC

2010

- (b)(1) USSC

2011

- (b)(1) USSC

2012

(U//FOUO) Demonstrated Attack Capabilities

(U) Shamoon Virus Infects Saudi Aramco

- World's largest crude exporter (U)
- More than 30,000 systems affected or rendered inoperable (U)
- (b)(1) USSC
-
-

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

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

(b)(1) USSC

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

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

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

(b)(1) USSC

~~(S//NF)~~ Chinese Threat Intent

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

Graphic is UNCLASSIFIED

(TS/(b)(1)/NF) STRATEGY

- (b)(1) USSC
-
-
-

(TS/(b)(1)/NF) CAPABILITY

- (b)(1) USSC
-

~~(S//NF)~~ Evolution of the Chinese Cyber Threat

Destruction ~~(S)~~

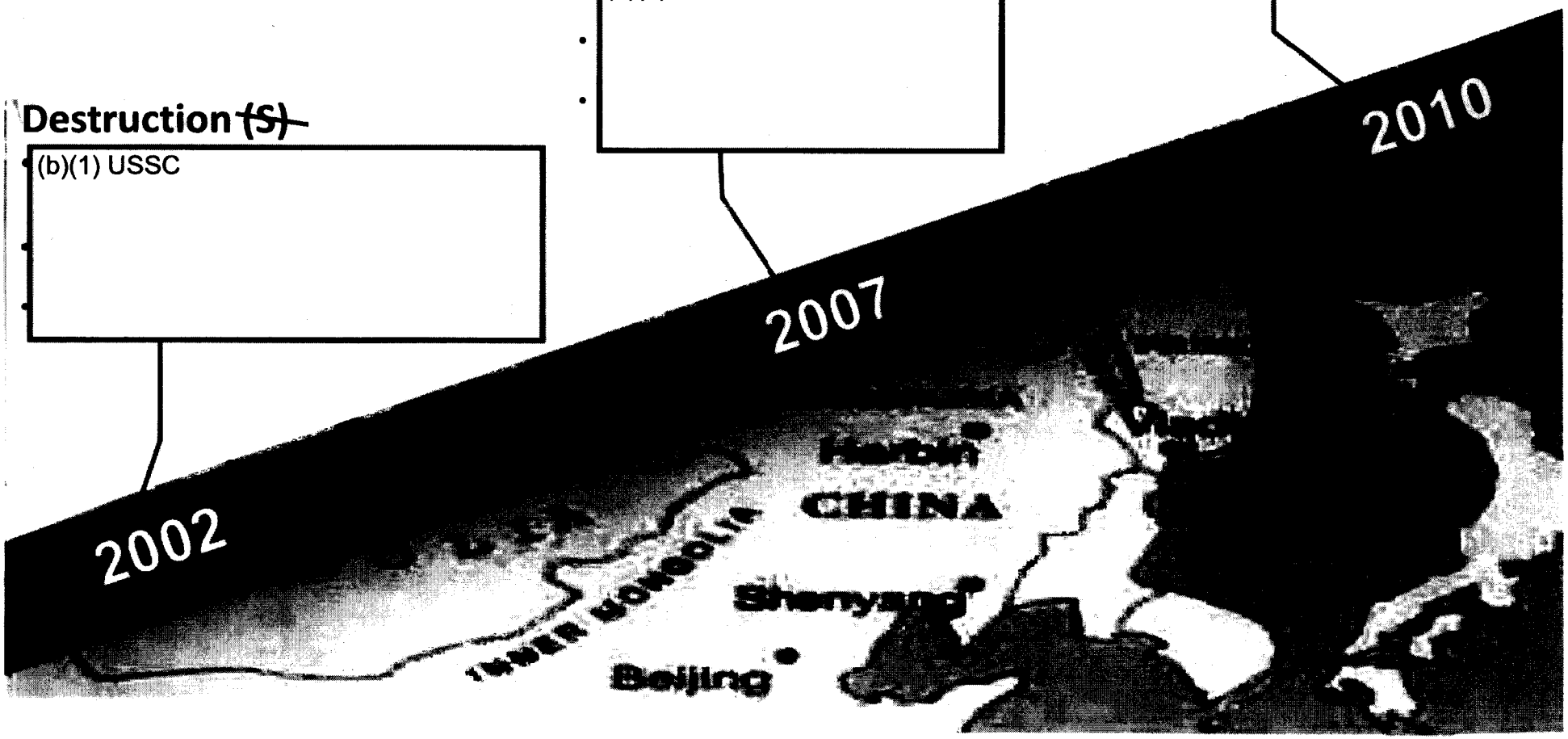
- (b)(1) USSC
-
-

Adaptation (U)

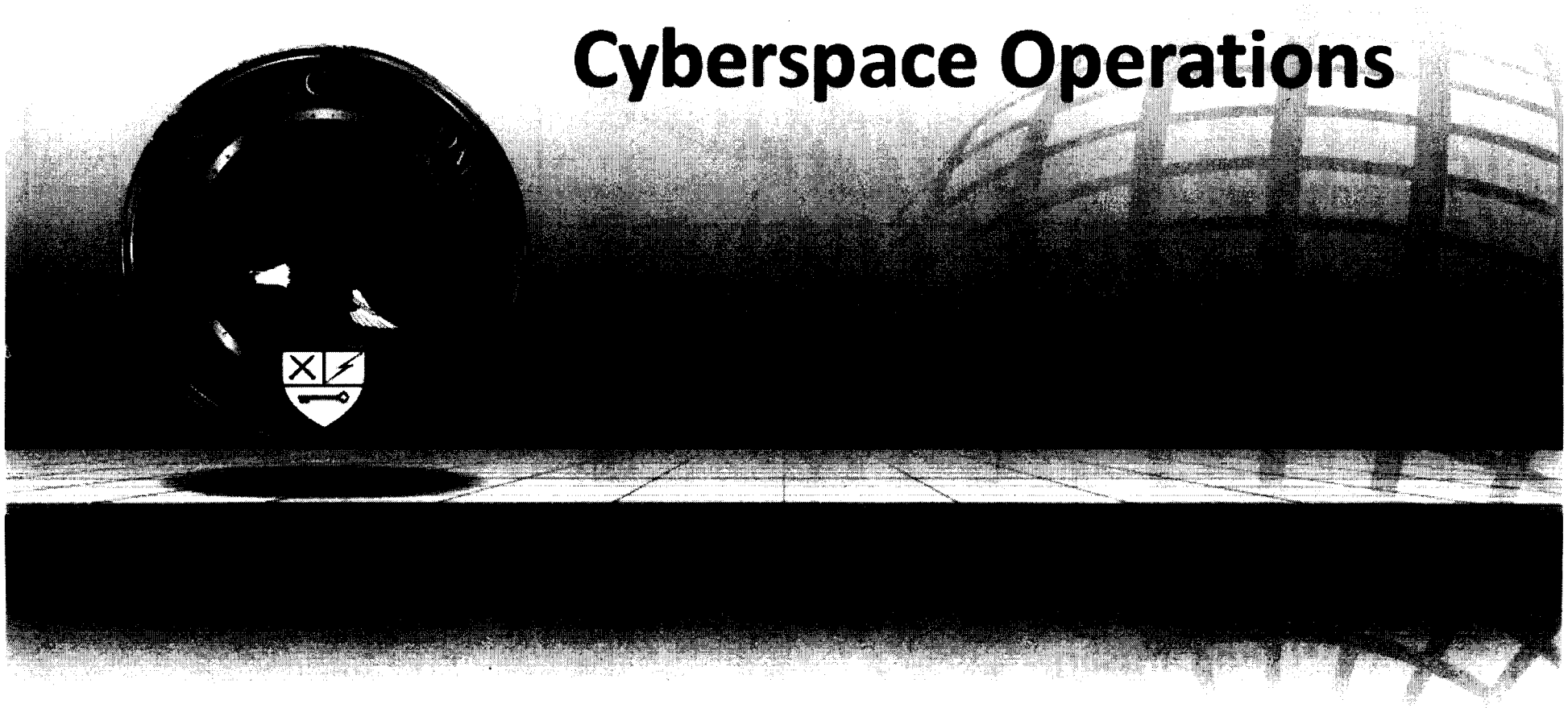
- (b)(1) USSC
-
-

Destruction ~~(S)~~

- (b)(1) USSC
-
-



Cyberspace Operations



USCYBERCOM Mission and Operations

USCYBERCOM Mission: *USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to:* ***direct the operations and defense of specified Department of Defense information networks*** *and; prepare to, and when directed,* ***conduct full spectrum military cyberspace operations*** *in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.*

Strategic Defense /Against Offensive

Operate and Defend

CCMD Support

[redacted]

[redacted]

[redacted]

(U) Organization: Supported Operations

Defend the Nation

(U) Concept of Operation

(U) SEE:

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

(b)(1) USSC

(U) BLOCK:

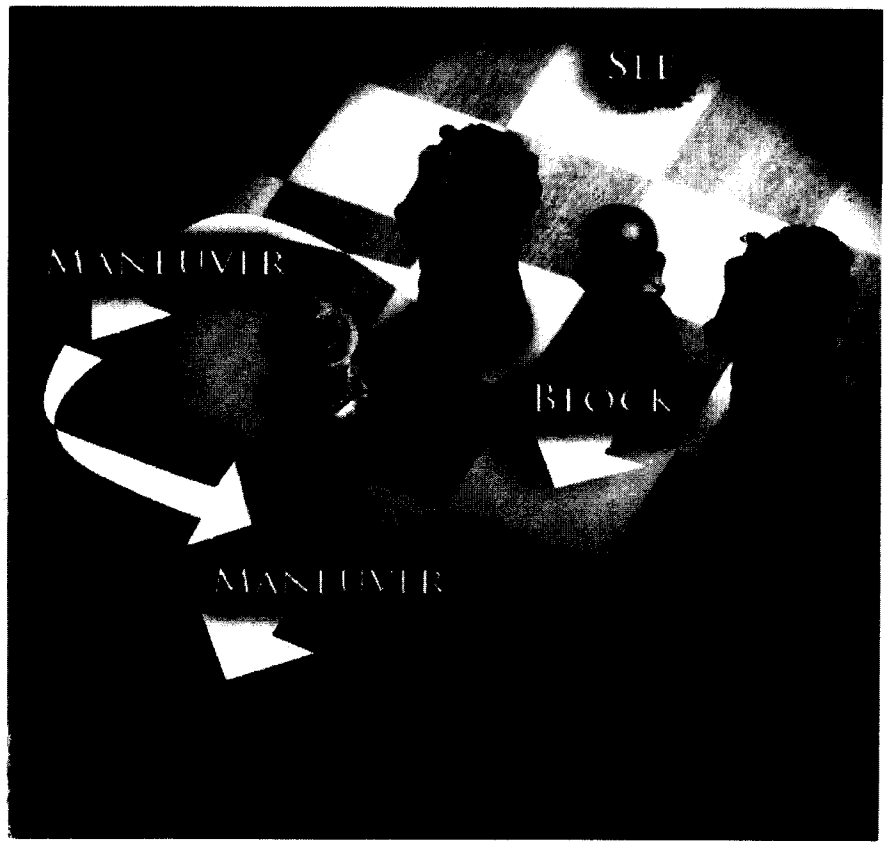
(U//~~FOUO~~) Employ both passive and active layered defenses to neutralize attacks in friendly, neutral, and adversary-controlled cyberspace.

(U)MANEUVER:

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

(b)(1) USSC

(U//~~FOUO~~) BE PREPARED TO STRIKE



Graphic: UNCLASSIFIED

(U) USCYBERCOM gives time to the President to make a decision on responsive actions.

Cyber C2 Model

(b)(1) USSC

Cyber Force Presentation (three basic types of Cyber Unit)

Cyber National Mission Battalion/Squadron

Mission: *See, Block, Maneuver in Red and Grey space to deny adversary objectives and, if authorized, strike to destroy the capability*

1 x C2 Element
- Provide C2 and management

5 x Cyber National Mission Teams (CNMT) (64 Pax each)
- Base unit for cyber operations
- Conduct OCO/DCO/DGO
- Sustained and surge operations
- Trained, certified, and fights as a team

5 x Direct Support Teams (DST) (39 pax each)
- Provides direct support to CNMTs
- Conduct intel and malware analysis
- Perform immediate tool development / modification and access maintenance
- Conduct target discovery / analysis
- Provide language analysis
- Planning and synchronization
- NSA initial weight to DTN DSTs, then shifting to CCMD support as capacity grows

Cyber Combat Mission Battalion/Squadron

Mission: *Target development in support of CCMD operations plans and, when authorized, the delivery of cyber effects against CCMD targets, followed by assessment of effects.* ***OPCON to CCMDs under current "Transitional" C2 model.***

1 x C2 Element
- Provide C2 and cyber management for CCMD (OPCON)

1-6 x Cyber Combat Mission Teams (CCMT) (64 Pax each)
- Base unit for offensive cyber operations
- (b)(1) USSC
- Large Scale ops CCMF has all CCMT specialties, others less
- Trained, certified, and fights as a team

1-2 x Direct Support Teams (39 Pax each)
- One DST per 3-5 CCMT
- More target region specific skills
- Perform immediate tool development / modification and access maintenance
- Conducts target discovery and analysis
- Provide language analysis
- Planning and synchronization

Cyber Protection Company/Troop

Mission: *Defense of the GIG and employing teams to assist outside the GIG when required & authorized*

Cyber Protection Company/Troop

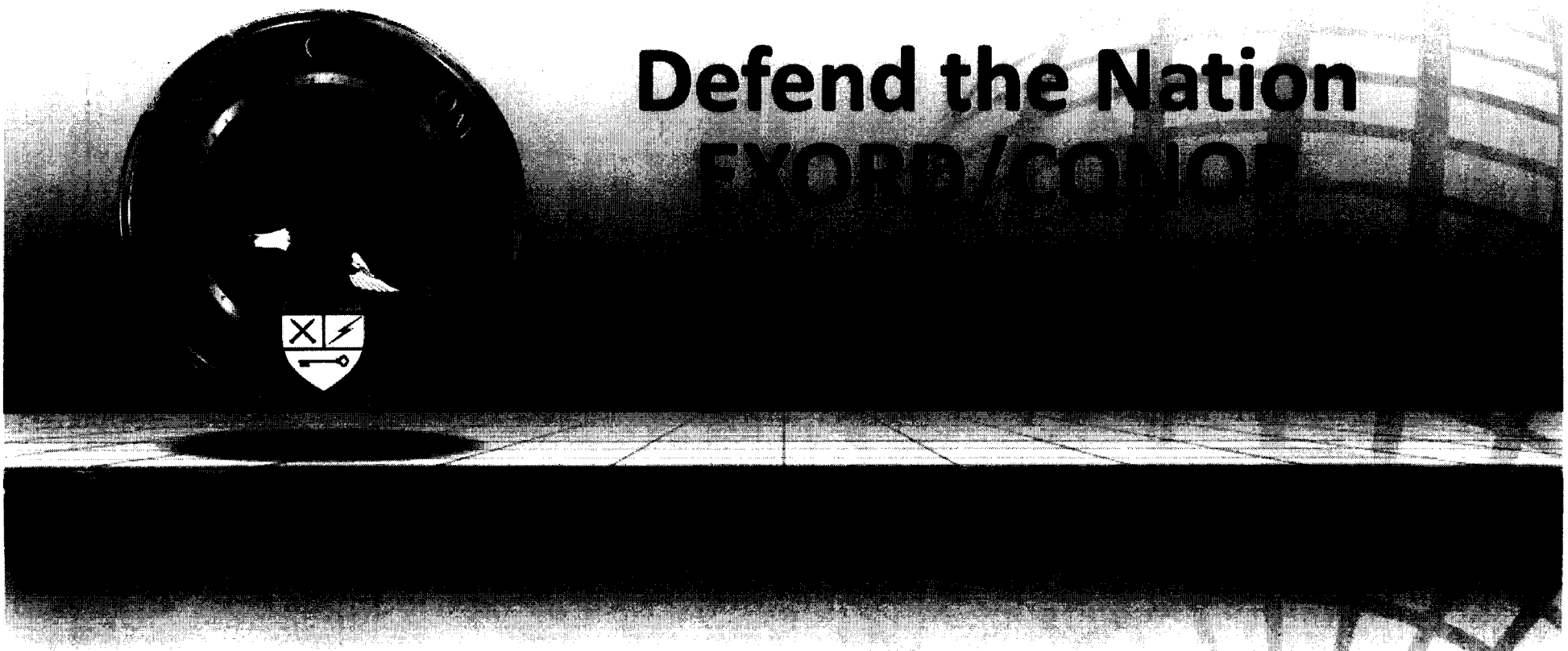
2-6 x Cyber Protection Platoons
- Each Platoon has its own organic C2 element
- Each Platoon has 5 squads (see below)
- Conduct CND; tips to CNA; Penetration testing
- Trained, certified, and operates as a team

5 x Protection Squads/Platoon
- Task organized, trained and certified
- Assesses Cyber Security Posture
- Bolsters Cyber Defenses
- Conducts Counter-Cyber Ops
- Performs Cyber Threat Emulation (CTE)
- Conducts intel and malware analysis

Force Planning Model

Supports USCYBERCOM Lines of Effort: Defense of the Nation, CCMD Contingency and Operational Plans, & Defending DoD Infrastructure

Defend the Nation -	CCMD Support -
(b)(1) USSC	



Classified By: ~~smzotti~~
Derived From: ~~USCYBERCOM SCG~~
Dated: 20111011
Declassify On: ~~20370901~~

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

Global Battlespace

(b)(1) USSC

Possible U.S. Responses to Iranian Cyber Attacks

(b)(1) USSC

(b)(1) USSC

Mission Statement

(b)(1) USSC

Commander's Intent

(b)(1) USSC

Situation: (b)(1) USSC

(b)(1) USSC

Possible Employment Scenario

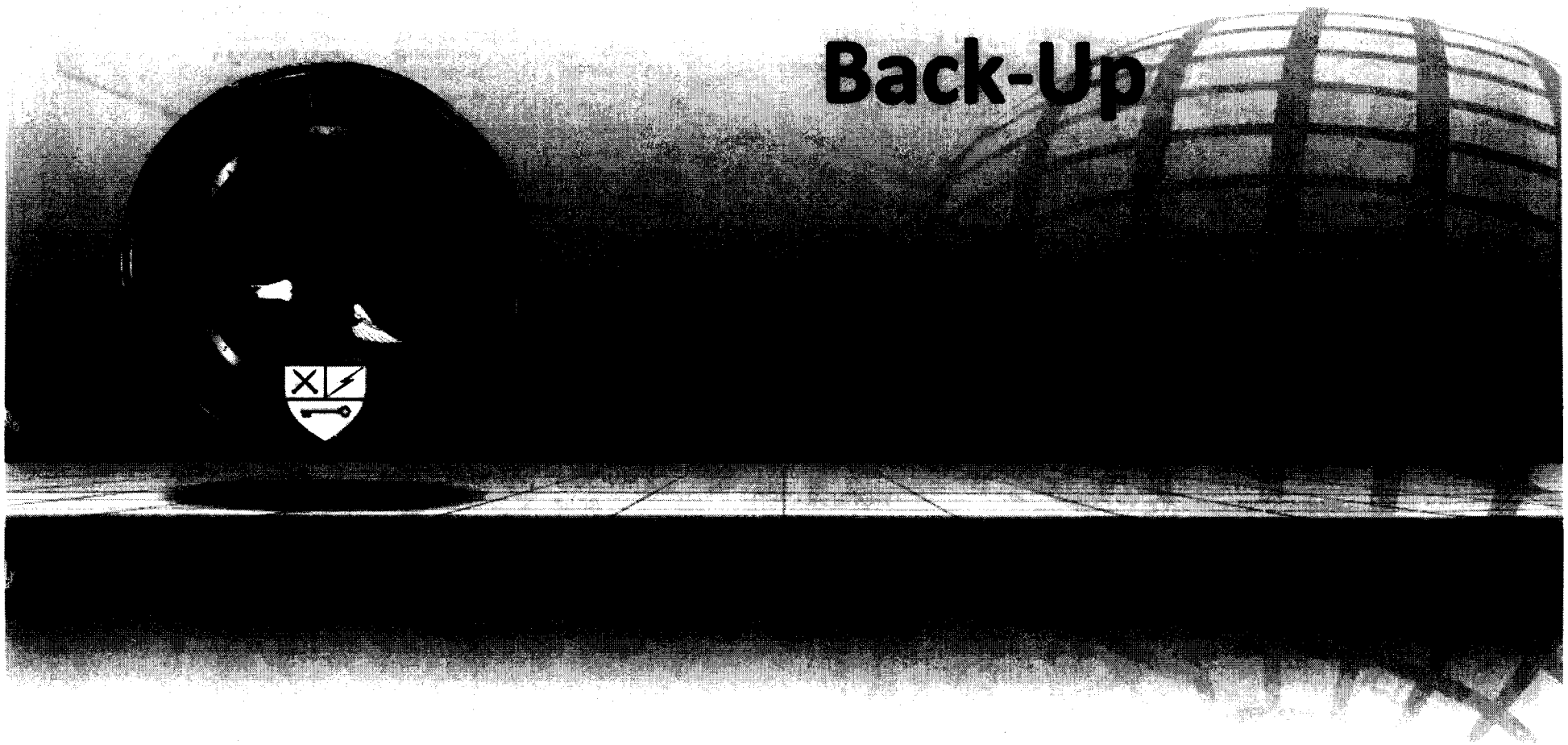
(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

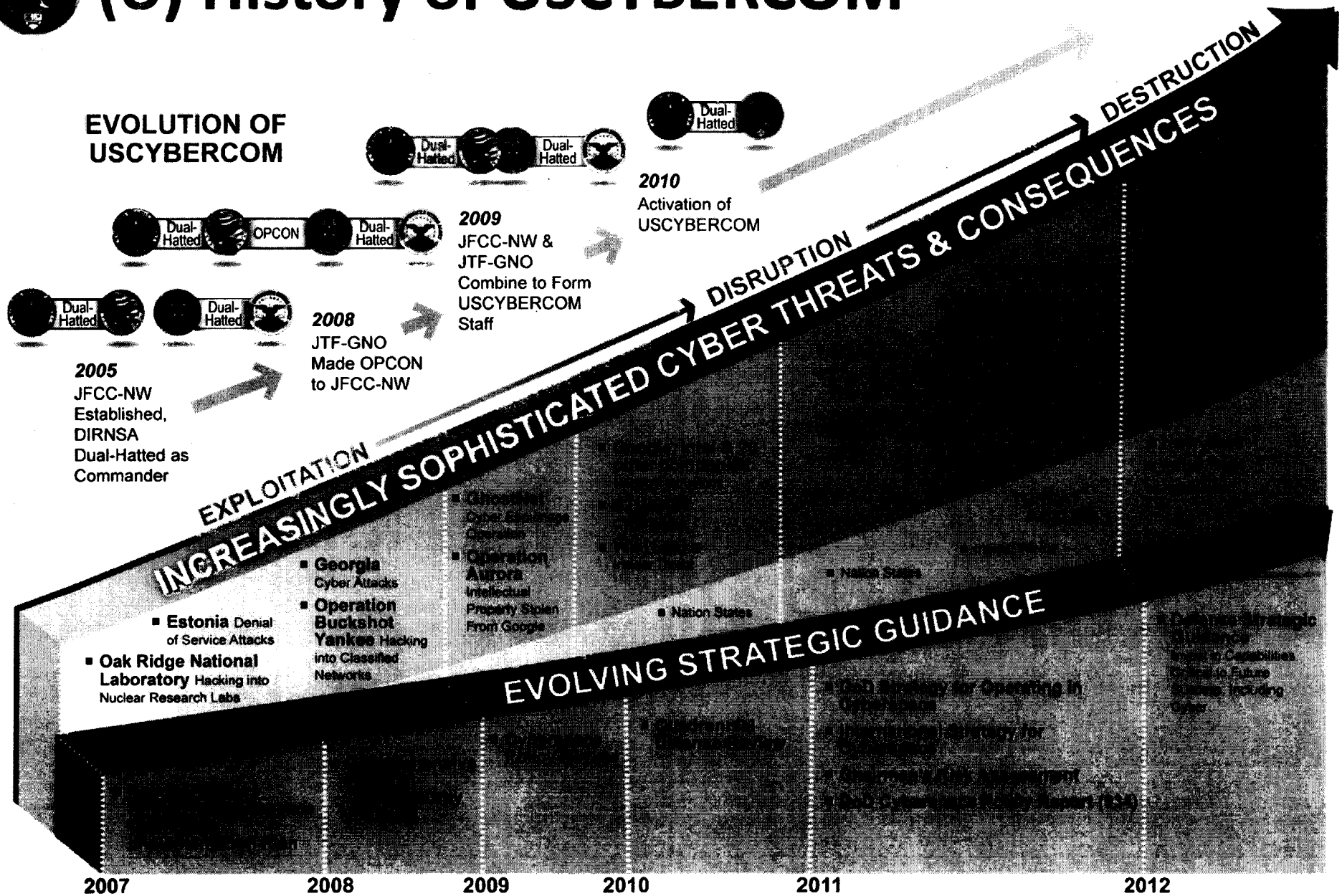
Questions?

Back-Up



(U) History of USCYBERCOM

Graphic: U//FOUO



Nature of Cyberspace

675 PETABYTES

265 BILLION

"13" MILLION

- Cyberspace: (DoD) "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."

  Source: Joint Pub 3-12

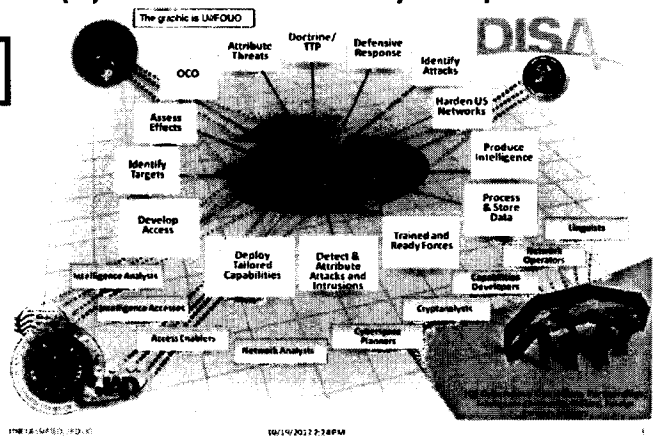
- However…
  - Manmade domain/ever changing/privately owned
  - Virtual
  - Programming code and protocols define rules of the domain
  - Environment/TTPs evolve at netspeed

(U) Success in this domain means being smarter, more creative, faster, and stealthier than our opponent.

(U) USCYBERCOM's Co-location with NSA and DISA: Optimized for Success

- (TS/(b)(1)/REL) (b)(1) USSC
  (b)(1) USSC
  - (b)(1) USSC
  -
- (U) Dual Hat: CDR USCYBERCOM and DIRNSA
  - Expedites decision making
  - Increases collaboration
  - Decryption
  - Linguistics
- (S//REL) (b)(1) USSC
  (b)(1) USSC
  - (b)(1) USSC
- (S//REL) (b)(1) USSC
- (U) Allows for joint cyber teams and development of a viable career path for cyber warriors
- (U) Enables information sharing, TTP development, operating concepts and technology development

(U) What it Takes to do Cyber Operations



Graphic: U//~~FOUO~~