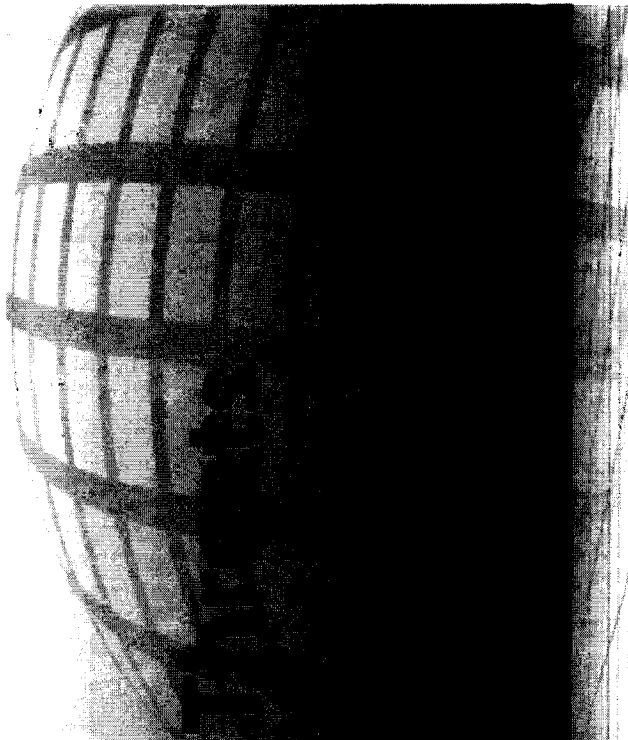
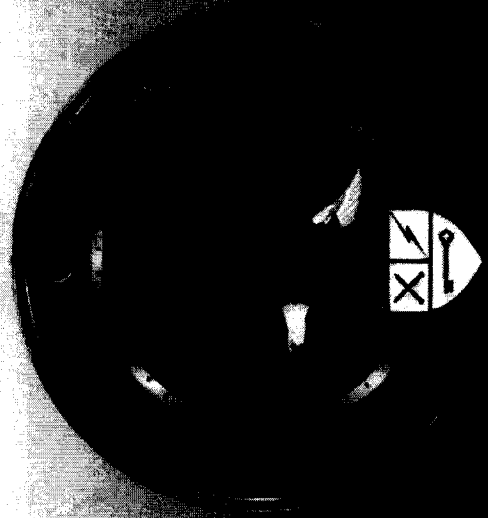


(b)(1)

SECRET



The overall classification of this brief is: **TOP SECRET**

(b)(1)

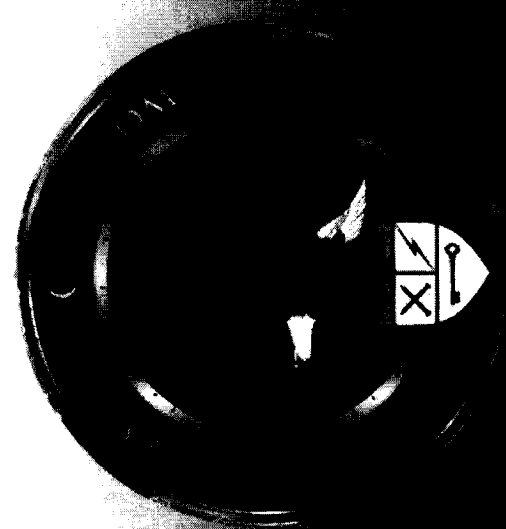
NOFORN Classified By: alperpe
Derived From: USCYBERCOM SCG
Dated: 20111011
Declassify On: 20371101

(b)(1)

UNCLASSIFIED

~~SECRET~~

TOP SECRET (b)(1) RETURN



Air Force Incidents

(b)(1)

UNCLAS

(b)(1)

SECRET

Cyber Threats to USAF Networks

(b)(1) USSC

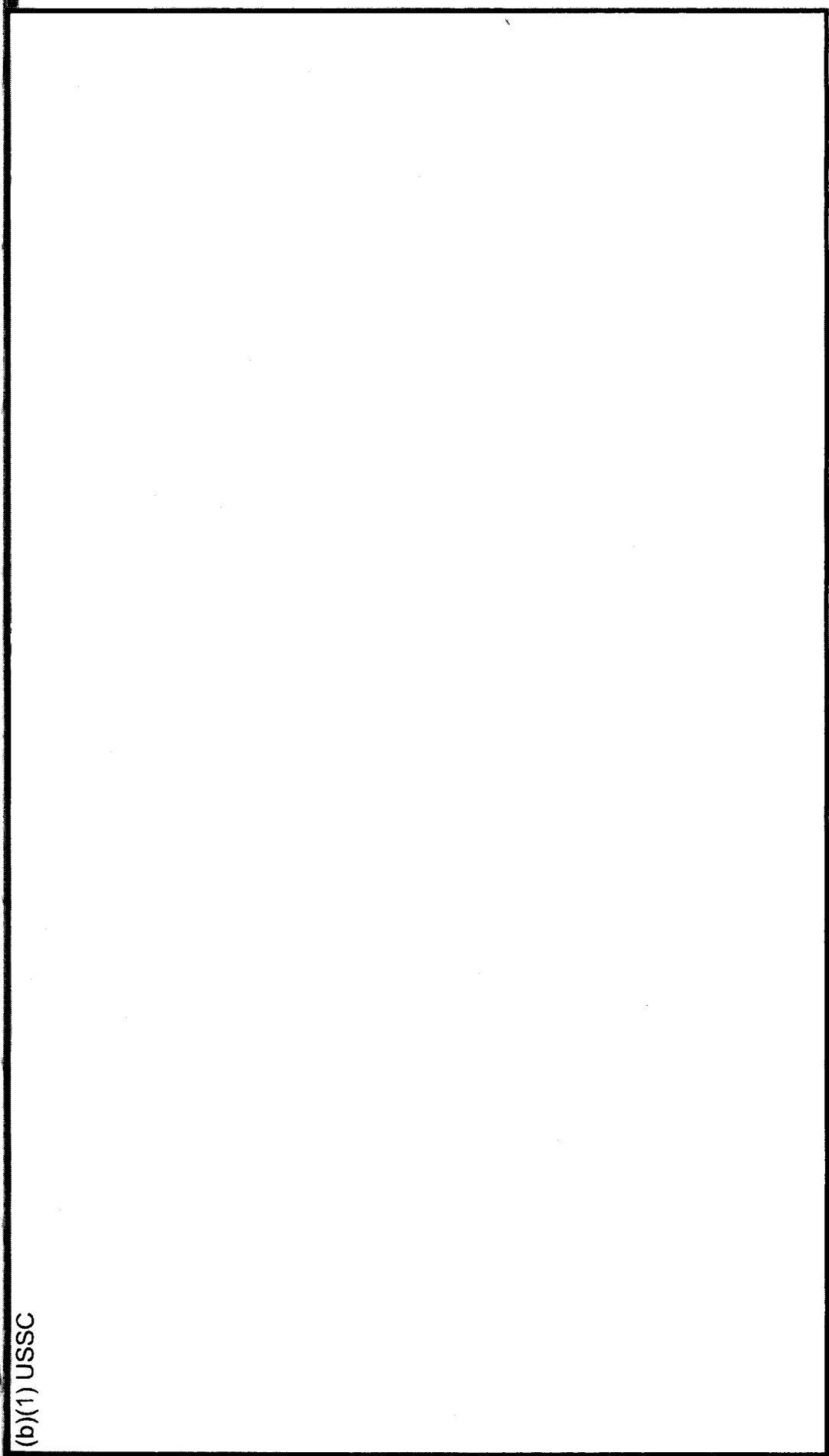
(b)(1)

SECRET

(b)(1)

Cyber Threats to USAF Supply Chain

(b)(1) USSC



(b)(1)

(b)(1)

Cyber Threats to USAF Platforms

(b)(1) USSC

(b)(1)

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

USE ONLY

(b)(1)



(b)(1)

UNCLASS

**SENATE ENGAGEMENT
16 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: tlpili
Derived From: USCYBERCOM SCG
Dated: 2011011
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.**

- **SAUDI ARAMCO**

- **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: 20380281

~~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

- 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
- LIBERTIES INCLUDE THE RIGHT TO PRIVACY & CIVIL RIGHTS ENSHRINED IN THE CONSTITUTION, TO AND WE ARE COMMITTED TO SUPPORTING THE PROTECTING OUR CRITICAL INFRASTRUCTURE DEFENDING OUR NATION IN CYBERSPACE AND NSA AND CYBERCOM REMAIN COMMITTED TO NETWORKS AND OUR INTELLECTUAL PROPERTY GREAT STARTING POINT TO PROTECTING OUR
- THE ISSUANCE OF THE EO LAST MONTH WAS A COMPLIANCE
- (U//FOUO) CIVIL LIBERTIES AND OVERSIGHT & ENGAGEMENT
- OF RESPONSIBILITY AND RULES OF
- WE CAN'T ACT QUICKLY WITHOUT CLEAR LINES CRITICAL INFRASTRUCTURE PROTECT FEDERAL NETWORKS AND DOMESTIC CYBERSECURITY AND HELP

**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
-
-
-

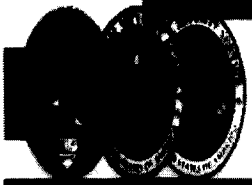
- ~~TOP SECRET~~ (b)(1) ~~NOFORN~~
- (TS) (b)(1) REL (b)(1) USSC
(b)(1) USSC
 - (b)(1) USSC
 -
 -
 - (TS) (b)(1) REL (b)(1) USSC
(b)(1) USSC
 - (b)(1) USSC
 -
 -

(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

(b)(1) USSC

Actors / Groups

US Sectors targeted

(b)(1)
USSC

**Leadership
awareness**

China Cyber Threat

<p>Characterization</p>	<p>(b)(1) USSC</p>
<p>Actors / Groups</p>	
<p>Primary Targets</p>	
<p>US Sectors targeted</p>	
<p>Stats from (b)(1) USSC</p>	
<p>Leadership awareness</p>	
<p>Trends / for</p>	
<p>(b)(1)</p>	

Iran Cyber Threat

(b)(1) USSC

Actors / Groups

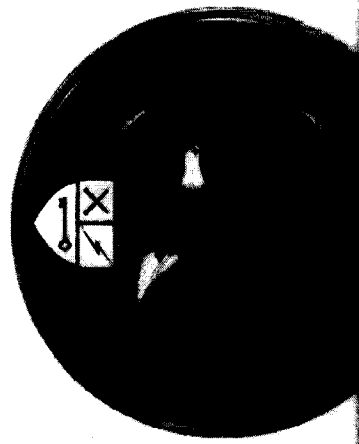
US Sectors targeted

(b)(1)
USSC

Leadership awareness

(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: 20370001~~

(b)(1)

(b)(1)

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

FBI, NSD, CRM,
USAO

NPPD, USSS,
ICE

USCYBERCOM, NSA,
DISA, DC3

SHARED SITUATIONAL AWARENESS ENABLING INTEGRATED OPERATIONAL ACTIONS

PROTECT | PREVENT | MITIGATE | RESPOND | RECOVER

(b)(1)



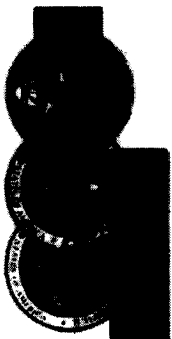
TAO Slides placeholder

(b)(1)

UNOFFICIAL

TOP SECRET

(b)(1)



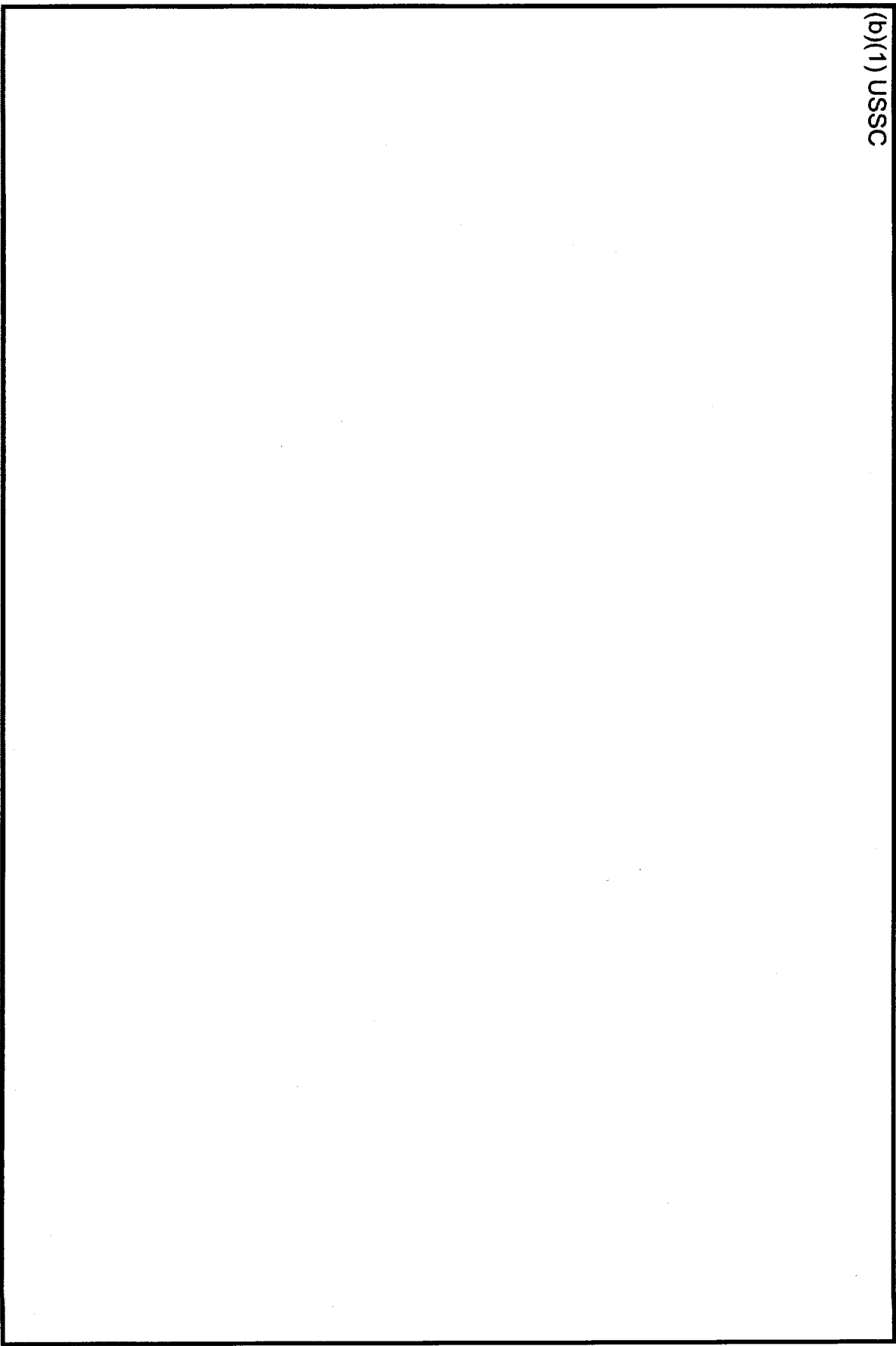
DDOS event vs

(b)(1) USSC

(b)(1)

UNCLASSIFIED

(b)(1) USSC

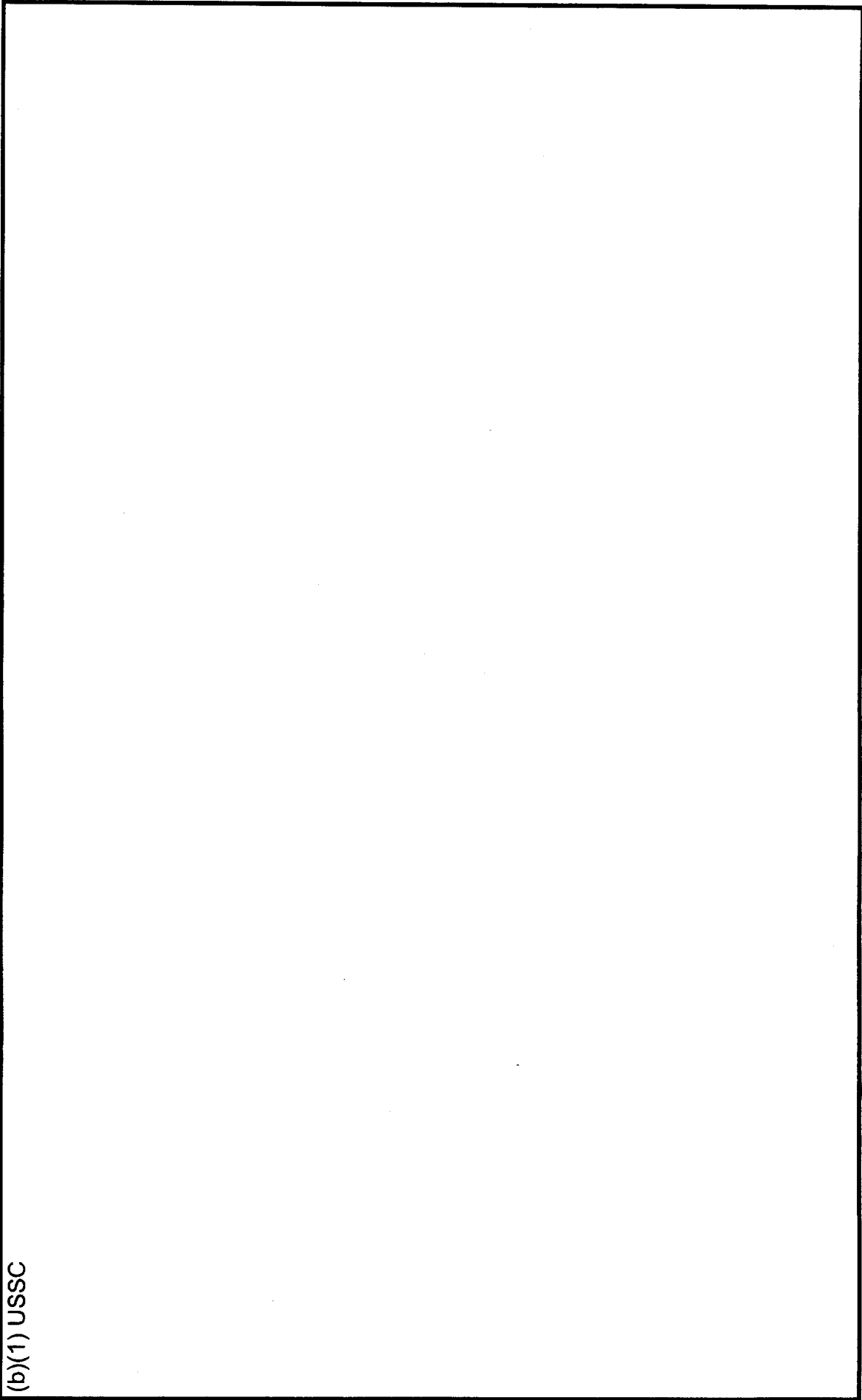


TOP SECRET

(b)(1)

The Anatomy of a DDos Attack

(b)(1) USSC



(b)(1)

How We Operate Globally to Defend the U.S.

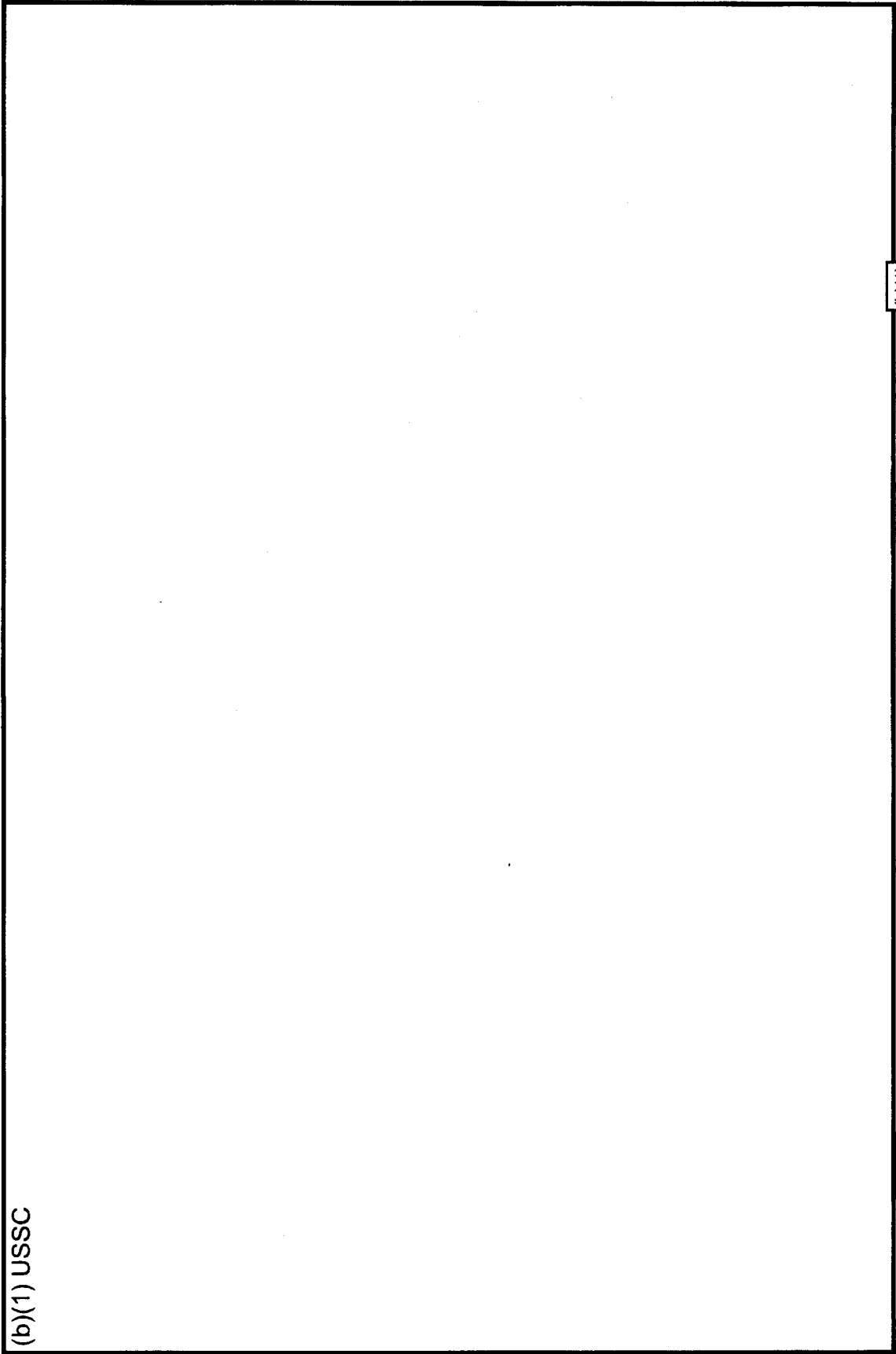
(b)(1) USSC

(b)(1) USSC

FOIA b(7) - (D)

(b)(1)

How Cyber Supports the Combatant Commander Action Against the Adversary



(b)(1) USSC

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

(b)(1)



Team Cyber Updates

(b)(1)

PROFORM

(b)(1) USSC



(b)(1) USSC



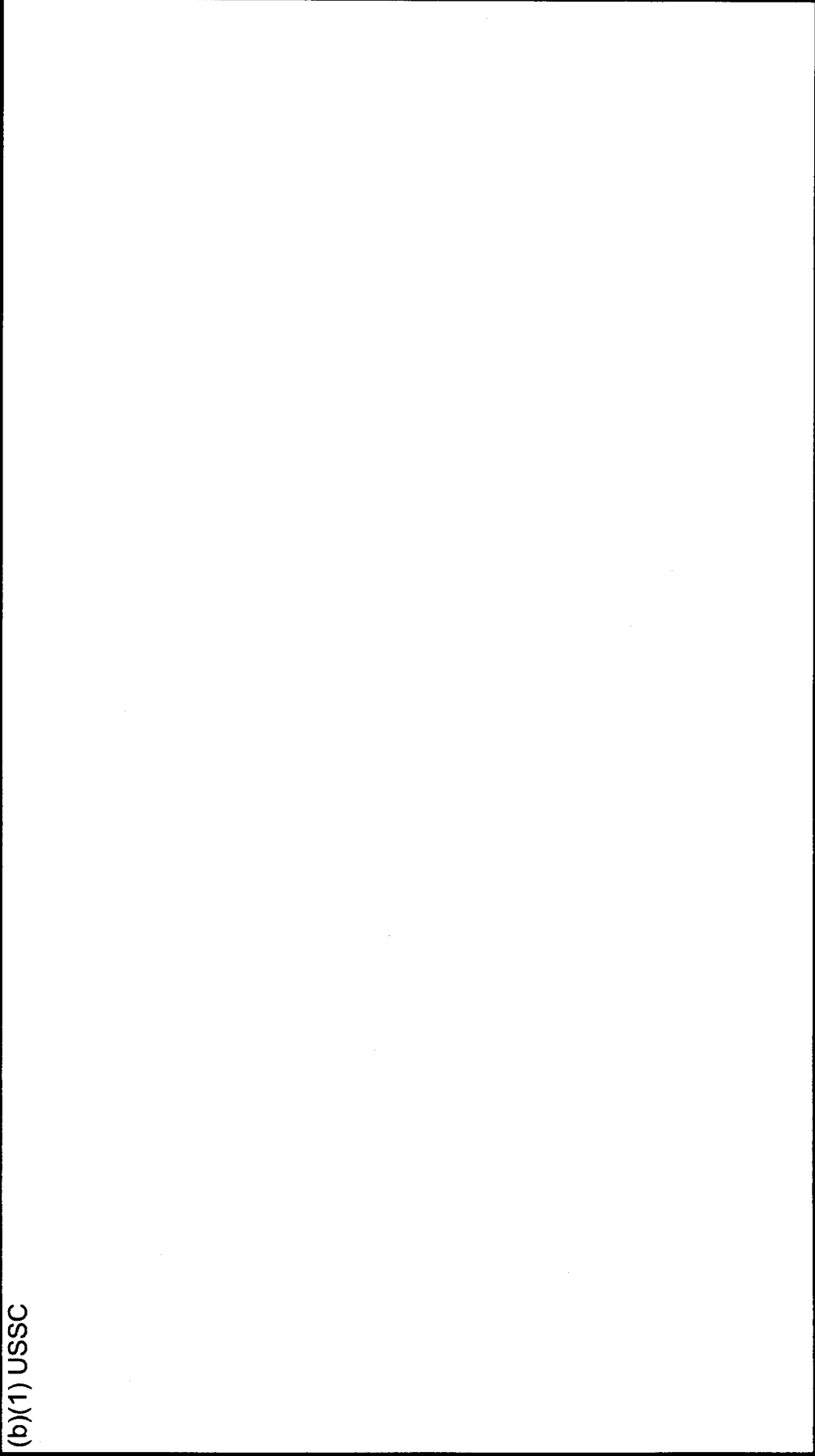
(b)(1)

(b)(1)



Team Cyber Updates

(b)(1) USSC



(b)(1)

(b)(1)

Team Cyber Updates

(b)(1) USSC

UNIFORM

(b)(1)

We Must Synchronize & Deconflict Operations

(b)(1) USSC



(b)(1) USSC

(b)(1)

USA, ET AL

(b)(1) USSC

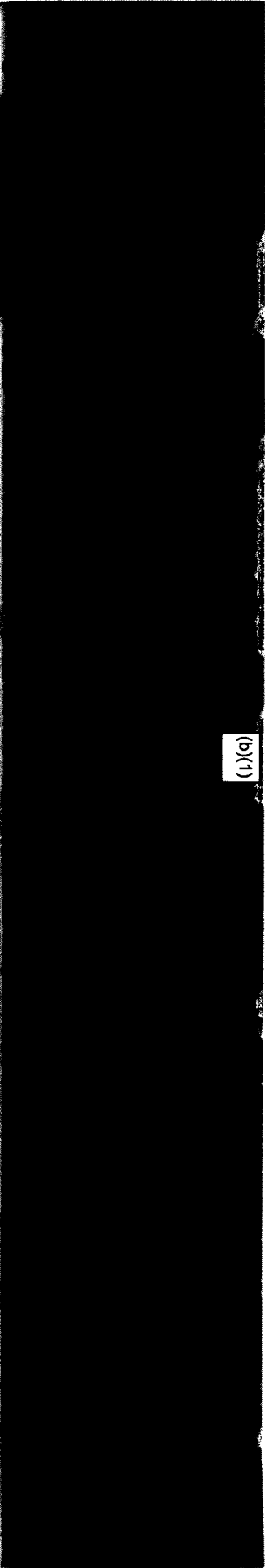
SECRET//K

(b)(1)

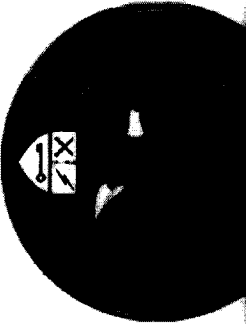
Cyber Mission Forces

(b)(1) USSC

(b)(1) USSC



(b)(1)



Questions?

UNCLASSIFIED



(b)(1)

(b)(1) USSC

(b)(1)

(b)(1)

TOP SECRET (b)(1) ALL TO USA, AUS, CAN, GBR, NZL

(b)(1)

(b)(1) USSC

(b)(1)

(b)(1) USSC

(b)(1)

(b)(1)

~~TOP SECRET~~

TOP SECRET

(b)(1)

REF TO USA, AUC, CAN, CDR, NZE

(b)(1) USSC



As of 31 March 2013

(b)(1)

KEY

(b)(1) USSC

(b)(1) USSC

(b)(1)

TOP SECRET

TOP SECRET

(b)(1)

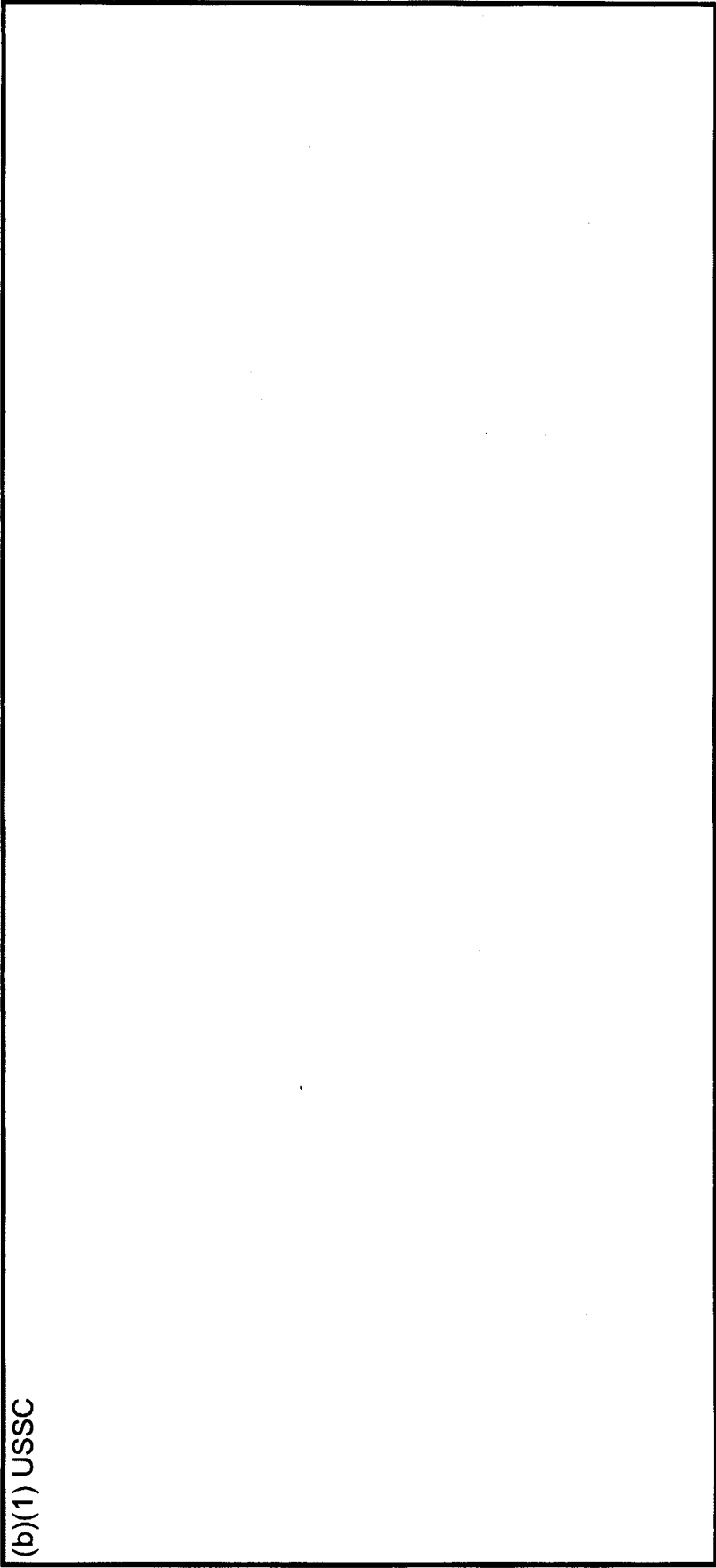
TOP SECRET



Response Options for the National Mission Fight

Countering the Adversary

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



(b)(1) USSC

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

02/07/2013 01:37 AM

PHOTOS: TS (b)(1) L TO USA, FVEY 6

U.S. Federal Cybersecurity Operations Team

National Roles and Responsibilities

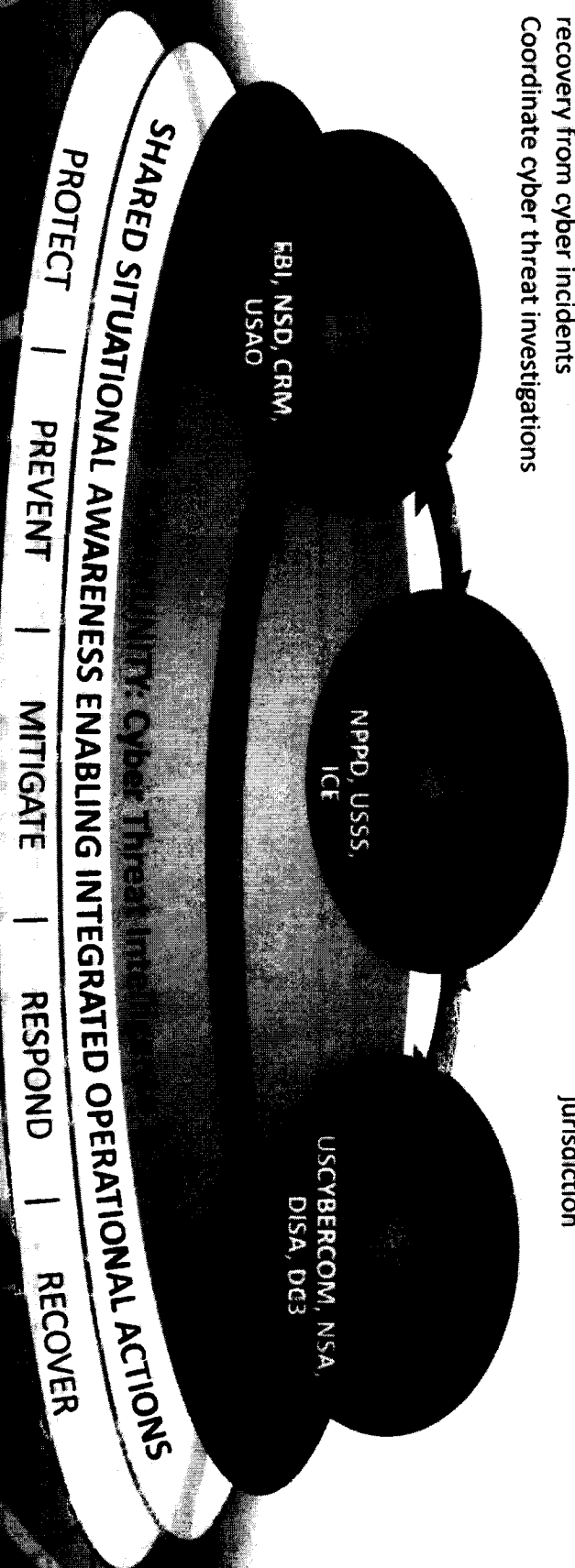
(b)(1)

DOJ

DHS

DoD

- 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
- Investigate cyber crimes under DHS's jurisdiction
- Investigate cyber crimes under military jurisdiction



(b)(1)



State-sponsored Threats

(b)(1) USSC

U.S. NETWORKS

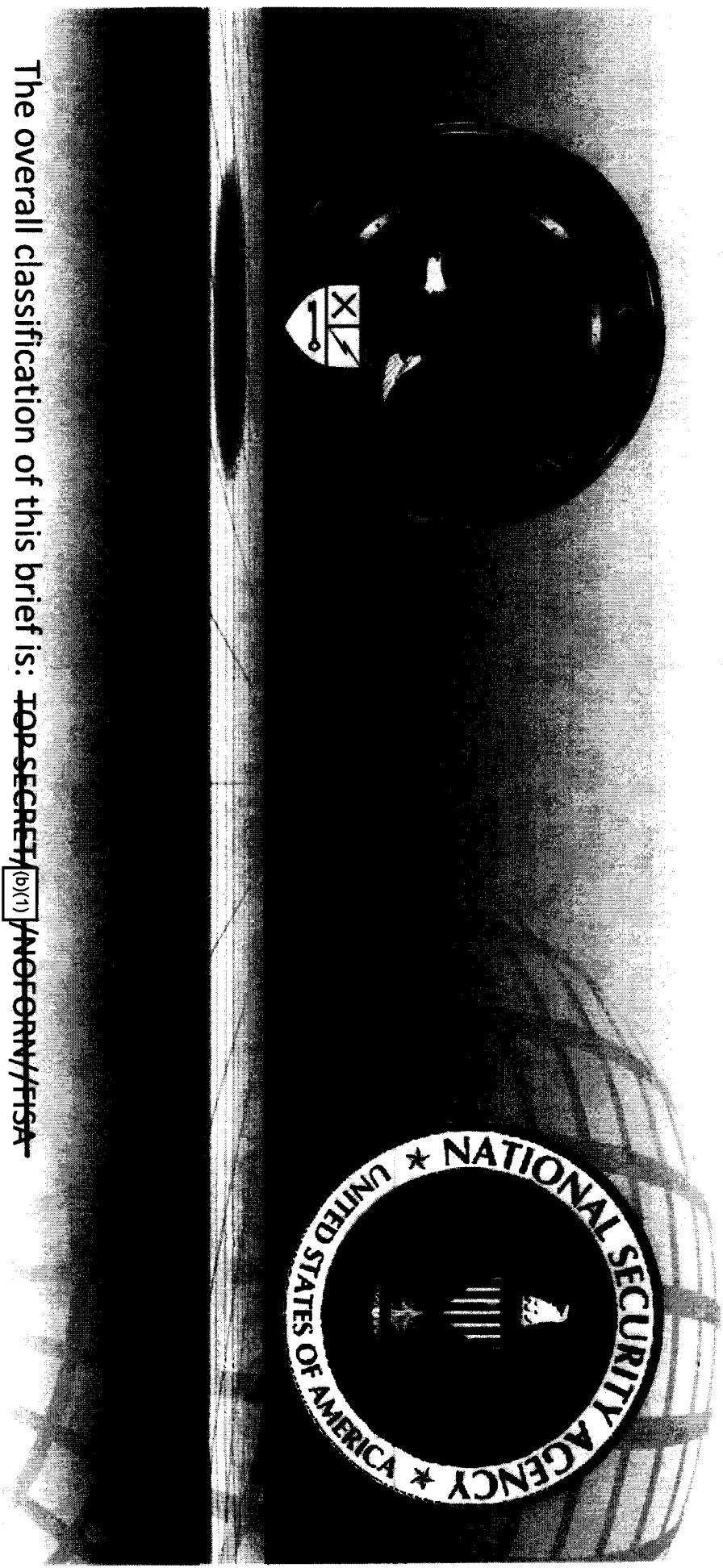
- U.S. Banking & Finance
- GOVERNMENT NETWORKS
- GOV INFO NETWORKS

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

(b)(1) USSC

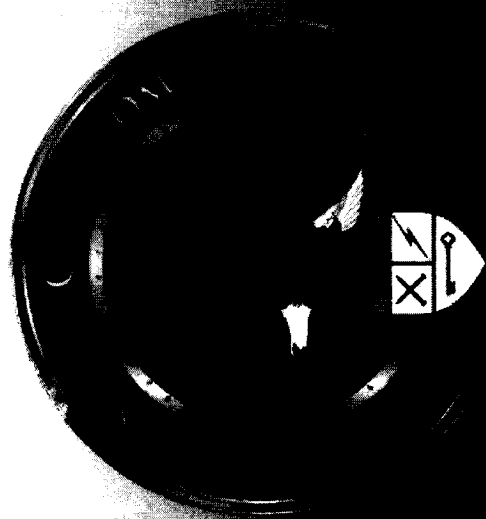
Cyberspace Security

Mr. Daniel



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

A Cyber Story: How NSA and CYBERCOM work together



HOW ^{(b)(1)} AND CYBER WORK TOGETHER
THE STORY BEGINS

ADDITIONAL

HOW [REDACTED] AND CYBER WORK TOGETHER

[REDACTED]
(b)(1) USSC

U.S. Decision Makers

INFORMATION



[REDACTED]
(b)(3) USSC

[REDACTED]
(b)(1) USSC

[REDACTED]
(b)(1) USSC

[REDACTED]
(b)(1) USSC

HOW ^{(b)(1)} AND CYBER WORK TOGETHER

(b)(1) USSC

INFORMATION
OPTIONS

(b)(3) USSC

[Redacted]

(b)(1) USSC

[Redacted]

(b)(1) USSC

[Redacted]

(b)(1) USSC

[Redacted]

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

INTEGRATION
OPTIMAL
SOLUTIONS

OPERATION

(b)(3) USSC

[Redacted]

(b)(1) USSC

[Redacted]

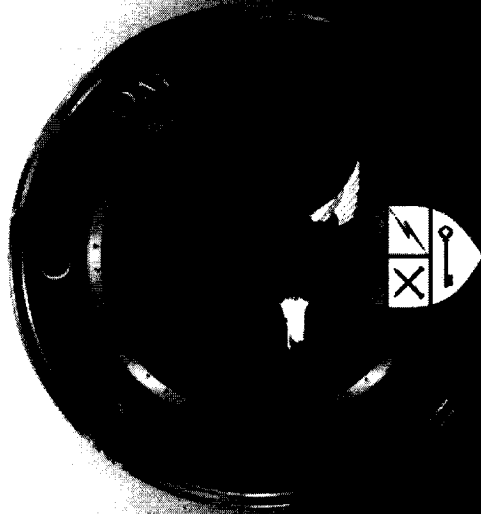
(b)(1) USSC

[Redacted]

(b)(1) USSC

[Redacted]

Cyber Threat





(S//NF)

(b)(1) USSC

• (TS (b)(1)/NF) (b)(1) USSC

• (TS (b)(1)/NF)

[Redacted]

(b)(1) USSC

• (TS (b)(1)/NF) (b)(1) USSC

[Redacted]

• (TS (b)(1)/NF) (b)(1) USSC

[Redacted]

(b)(1) USSC



Graphic is UNCLASSIFIED

(U) STRATEGY

(b)(1) USSC

[Redacted]

(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)

(b)(1) USSC

(S//REL)

(b)(1) USSC

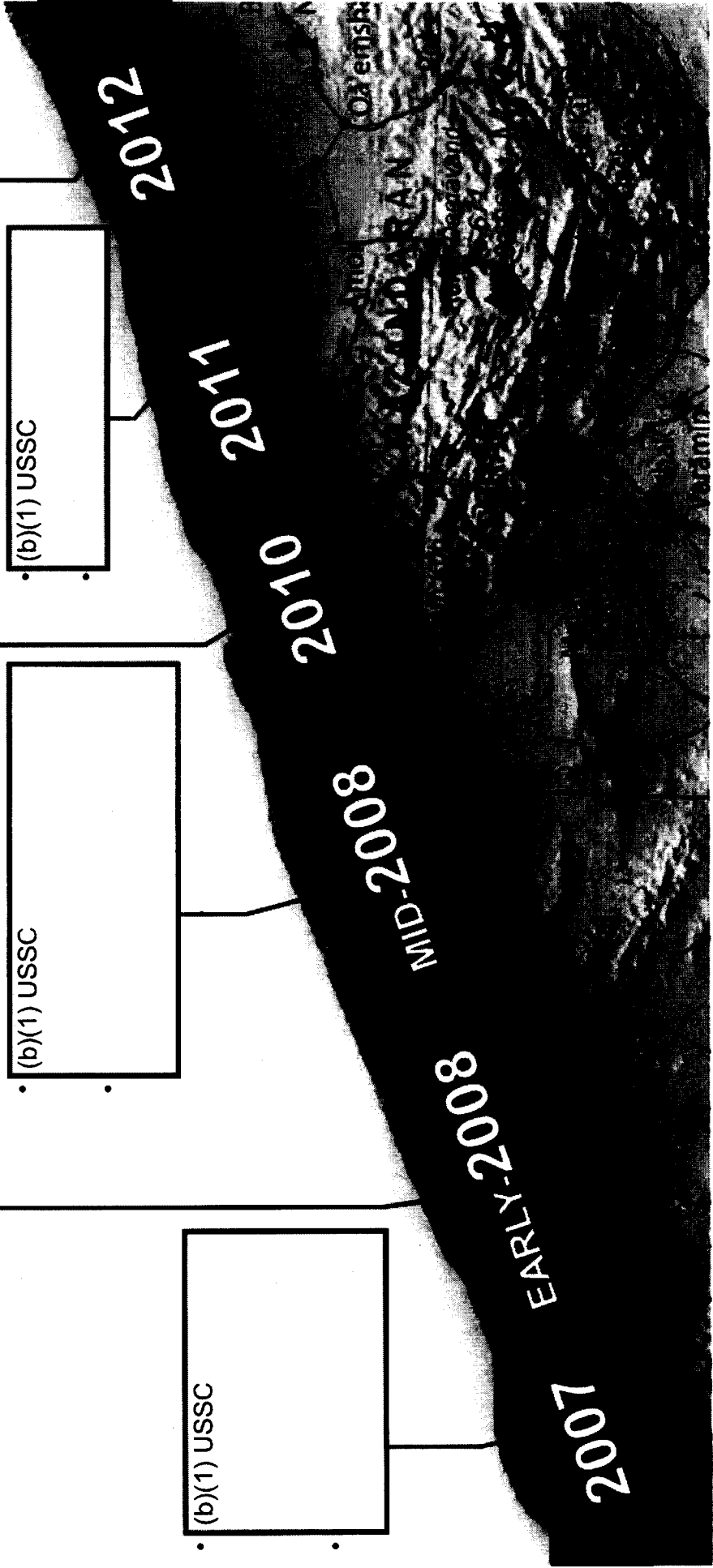
(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC





(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

(b)(1)



(S//NF) Chinese Threat Intent

- (TS//NF) /NF)
- (TS//NF) /NF)
- (TS//NF) /NF)
- (TS//NF) /NF)
- (TS//NF) /NF)

(b)(1) USSC



Graphic is UNCLASSIFIED

(TS//NF) STRATEGY

(TS//NF) CAPABILITY

(b)(1) USSC

(b)(1) USSC

(b)(1)

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

~~Destruction (S)~~

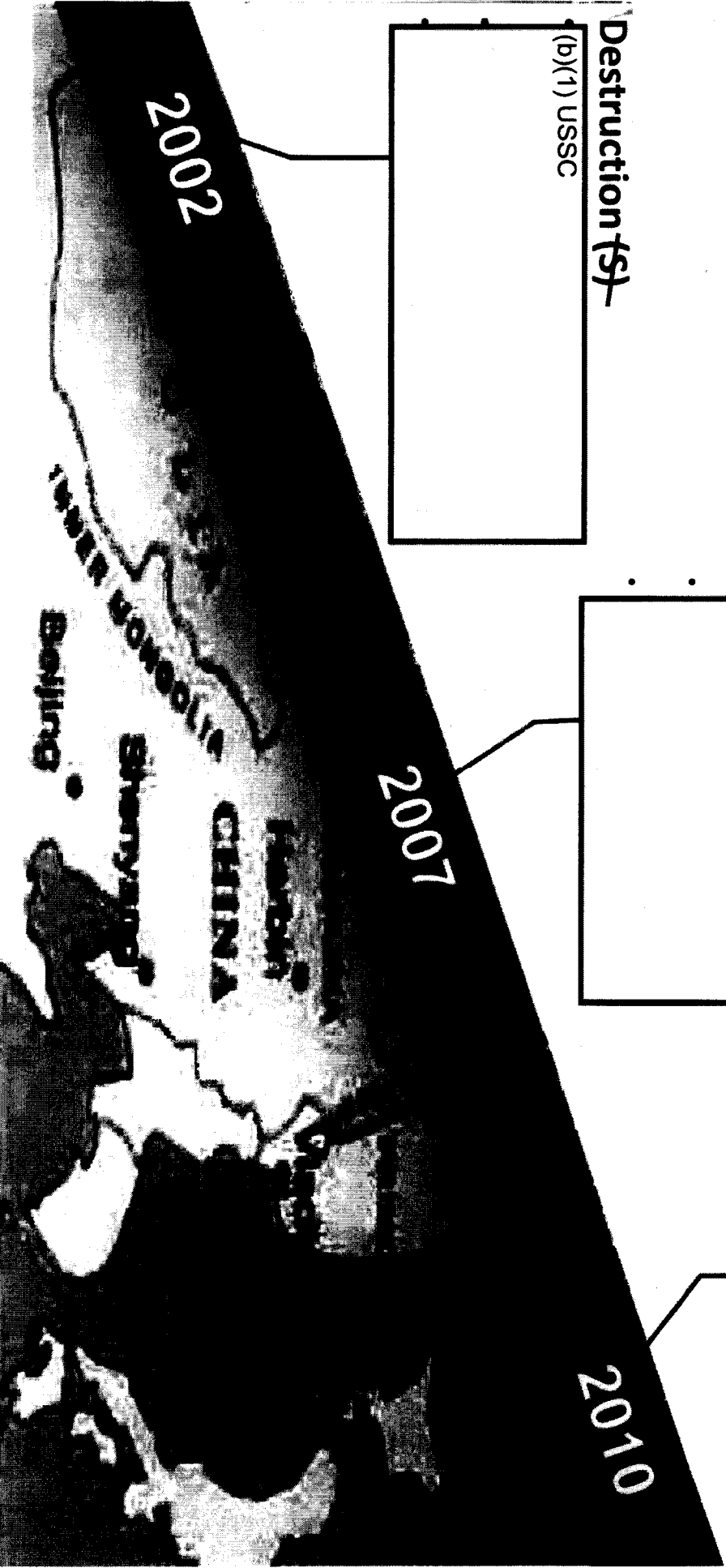
• (b)(1) USSC

Adaptation (U)

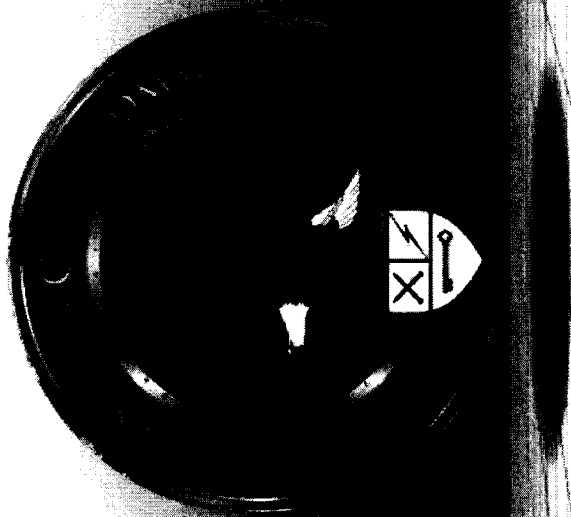
• (b)(1) USSC

~~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

Assess and Counter Offensive

Operate and Defend

Command Support



(U) Organization: Supported Operations

Defend the Nation

(U) Concept of Operation

(U) SEE:

(S//REL) [REDACTED] (b)(1) USSC

[REDACTED] (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) [REDACTED] (b)(1) USSC

[REDACTED] (b)(1) USSC

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



Graphic: UNCLASSIFIED

(U//~~FOUO~~) USCYBERCOM always time to the President to make a decision on responsive actions.

Cyber-C2 Model

(b)(1) USSC