United States Cyber Command

Delivering Outcomes through Cyberspace

CAPT Jody Grady, USN
USCYBERCOM LNO to USPACOM
Motivated by MISSION | Powered through PARTNERSHIPS | Oriented toward OUTCOMES
Organization
Organizational Structure

CNMF
Cyber National Mission Force

JFHQ-DODIN
Joint Force Headquarters-DOD Information Networks

AFCYBER
Air Forces Cyber

ARCYBER
Army Cyber Command

FLTNCYBER
Fleet Cyber Command

MARFORCYBER
Marine Corps Forces Cyberspace Command

CGCYBER
Coast Guard Cyber Command

133 Cyber Mission Force Teams are assigned to these Commands

National Mission Forces
National Mission and Support Teams

Combat Mission Forces
Combat Mission and Support Teams

Cyber Protection Forces
Cyber Protection Teams
History
Cyberspace Incidents

Increasingly Sophisticated Cyber Threats & Consequences

2011
- Nasdaq network infiltrated by unknown actors
- RSA network intrusion
- Oak Ridge National Laboratory phishing using social engineered emails

2012
- Shamoon Virus infected over 30,000 computers overwriting data and disrupting operations at Aramco
- DDoS Attacks
  - NY Stock Exchange
  - Bank of America
  - Capital One
  - BB&T
  - JP Morgan Chase
- Apple and Facebook hacked by China
- Twitter hijack impacts US stocks
- Network Intrusion Wallstreet Journal and New York Times
- DDoS of Republic of Korea’s main ISP and a cyber attack disabling 42,000 computers

2013
- Anonymous hacked North Korea published 15,000 login/passwords
- Target Data Breach up to 70 million bank cards compromised
- Heartbleed Bug ~66% of all Internet traffic potentially exposed to data leaks
- Sandworm zero-day exploit against NATO, EU, telecom, and energy sectors
- US Casino hit with destructive cyber attack
- North Korea data deletion attack against US Sony Pictures
- OPM breach ~4 million individuals’ PII potentially affected

2014
- USCENTCOM’s Twitter and YouTube accounts hacked by Cyber Caliphate
- Anthem health insurer compromised 80+ million SSNs stolen
- OPM Breach ~21 million individuals’ PII potentially affected

2015
- USCENTCOM's Twitter and YouTube accounts hacked by Cyber Caliphate
- Anthem health insurer compromised 80+ million SSNs stolen
- OPM Breach ~21 million individuals’ PII potentially affected

Increasingly Sophisticated Cyber Threats & Consequences

Cyberspace Incidents

- Shamoon Virus infected over 30,000 computers overwriting data and disrupting operations at Aramco
- DDoS Attacks
  - NY Stock Exchange
  - Bank of America
  - Capital One
  - BB&T
  - JP Morgan Chase
- Apple and Facebook hacked by China
- Twitter hijack impacts US stocks
- Network Intrusion Wallstreet Journal and New York Times
- DDoS of Republic of Korea’s main ISP and a cyber attack disabling 42,000 computers
- Anonymous hacked North Korea published 15,000 login/passwords
- Target Data Breach up to 70 million bank cards compromised
- Heartbleed Bug ~66% of all Internet traffic potentially exposed to data leaks
- Sandworm zero-day exploit against NATO, EU, telecom, and energy sectors
- US Casino hit with destructive cyber attack
- North Korea data deletion attack against US Sony Pictures
- OPM breach ~4 million individuals’ PII potentially affected
- USCENTCOM’s Twitter and YouTube accounts hacked by Cyber Caliphate
- Anthem health insurer compromised 80+ million SSNs stolen
- OPM Breach ~21 million individuals’ PII potentially affected
Evolving with the Threat

**US Cyber Command**
- Activated as a sub-unified command under US Strategic Command
- Full-spectrum military operations

**Cyber Mission Force Build**
- National Mission Forces
- Combat Mission Forces
- Cyber Protection Forces

**2010**
- RSA Compromised

**2011**
- Shamoon Virus
- Destructive attack
- DDoS attacks on banks

**2012**
- Navy and Marine Corps Intranet Intrusion

**2013**
- Target, OPM Data breach
- Heartbleed
- Open SSL vuln.
- Sony Intrusion

**2014**
- JFHQ-DODIN activated

**2015**

**2016**
Commander’s Vision

MISSION

- Ensure Department of Defense mission assurance
- Deter or defeat strategic threats to US interests and infrastructure
- Achieve Joint Force Commander objectives

IMPERATIVES

- Defend the nation’s vital interests in cyberspace
- Operationalize the cyber mission set
- Integrate cyberspace operations in support of joint force objectives
- Accelerate full-spectrum capacity and capability development

ENABLERS

- Demonstrated value and credibility
- Defined command and control
- The other C2: cooperation and collaboration
- Professionalized force
- Acquisition agility
Motivated by MISSION
US Cyber Command is an agile, innovative, and accountable organization supporting the Department of Defense’s mission in cyberspace by:

- Ensuring Department of Defense mission assurance
- Deterring or defeating strategic threats to US interests and infrastructure
- Achieving Joint Force Commander objectives
Command Objectives & Lines of Effort

- Ensure Department of Defense mission assurance
- Deter or defeat strategic threats to US interests and infrastructure
- Achieve Joint Force Commander objectives

PROTECT US cyberspace interests
PROJECT power in & through cyberspace
PARTNER with interagency & partner nations
Strategic Guidance

National Security Strategy 2015

International Strategy for Cyberspace 2011

Department of Defense Cyber Strategy 2015

Commander’s Vision and Guidance for US Cyber Command 2015
Oriented toward OUTCOMES
Cyber Mission Force Teams

National Mission Forces
Counter Cyberspace Attacks
21 Teams

Combat Mission Forces
Focused On Combatant Command Requirements
44 Teams

Cyber Protection Forces
Defend and Secure DOD Infrastructure + Support for Protecting DOD Networks
68 Teams

133 Total Teams 6,000+ People
National Mission Forces

Defend the Nation by seeing adversary activity, blocking attacks, and maneuvering to defeat them.
Combat Mission Forces

Conduct military cyberspace operations in support of the joint warfighter
Cyber Protection Forces

Defend the Department of Defense Information Networks and protect priority missions
Operations

→ Collaborating with all levels of government

→ Sharing information with US Government, private sector and international partners

→ Stopping intrusions into the Department of Defense Information Networks
Operations

- Deterring cyber threats
- Attributing adversary activities
- Building capacity and capability for cyberspace operations
- Countering intellectual property theft for Department of Defense
Powered through PARTNERSHIPS
Powered through PARTNERSHIPS

→ US Government
→ Industry
→ Allies

→ Academia
→ Foreign Partners
US Federal Cybersecurity Operations Team

National Roles and Responsibilities

DOJ/FBI
Lead for Investigation and Enforcement

DHS
Lead for Protection

DOD
Lead for National Defense

Coordinate with Public, Private, and International Partners

INTELLIGENCE COMMUNITY: Cyber Threat Intelligence & Attribution

SHARED SITUATIONAL AWARENESS ENABLING INTEGRATED OPERATIONAL ACTIONS

PROTECT | PREVENT | MITIGATE | RESPOND | RECOVER
Nature of the Domain
Our Interconnected World

- Critical Infrastructure
- US Government
- Financial Sector
- US & Foreign Citizens
- Power Grid
- Criminal Elements
- Terrorists
- Hacktivists
- Data
- Voice
- TV
- Radio
- Satellite

Critical Infrastructure

US Government

Financial Sector

US & Foreign Citizens

Power Grid

Criminal Elements

Terrorists

Hacktivists
Complexity of Cyberspace

- Social Media
- Mobile
- Cloud
- Internet of Things
- Wearables
The cyberspace mission is vital for the security of our country and, for that matter, the security of our economy and our people in their individual lives, because cyber touches all aspects of their lives.

– Ashton Carter
United States Secretary of Defense
13 Mar 2015 Visit to USCYBERCOM
Questions?