Iowa Air National Guard Cyber Protection Team

Maj Brian Dutcher

Director of Operations, 168th Cyber Operations Squadron

Overview

- Cyber Mission Force
- Defensive Cyber Operation Capabilities
- Air National Guard Cyber Protection Teams
- 168th Cyber Operations Squadron Domestic Operations
- Domestic Ops Example - Cyber Shield 2016
- Power of the Iowa Citizen Airmen

DOD Information Global Network Operations

*Network focused/threat agnostic

Defensive Cyberspace Operations (DCO)

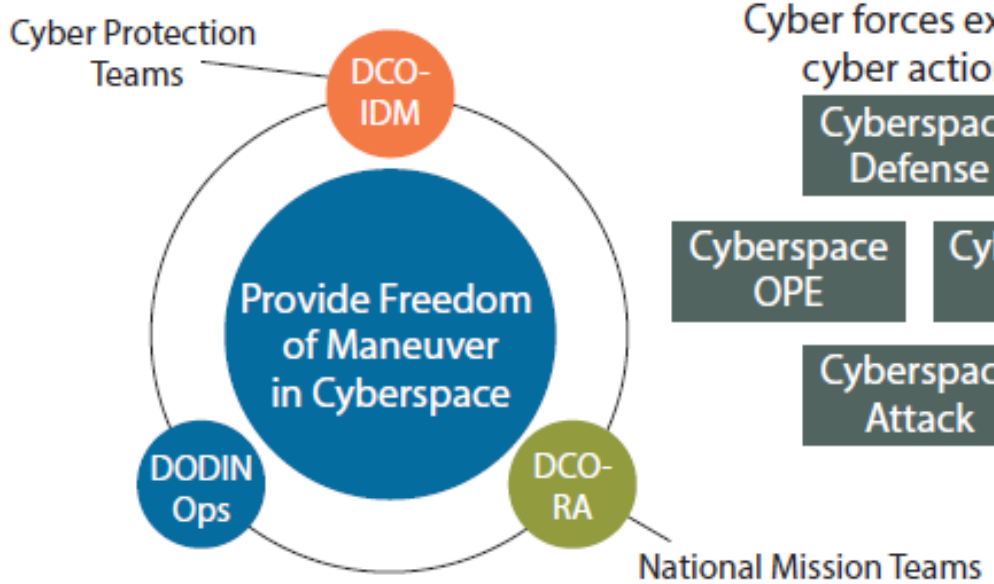
DCO–Internal Defensive Measures (DCO-IDM)

DCO–Response Actions (DCO-RA)

*Mission focused/threat specific

Offensive Cyberspace Operations

* Project power in and through cyberspace



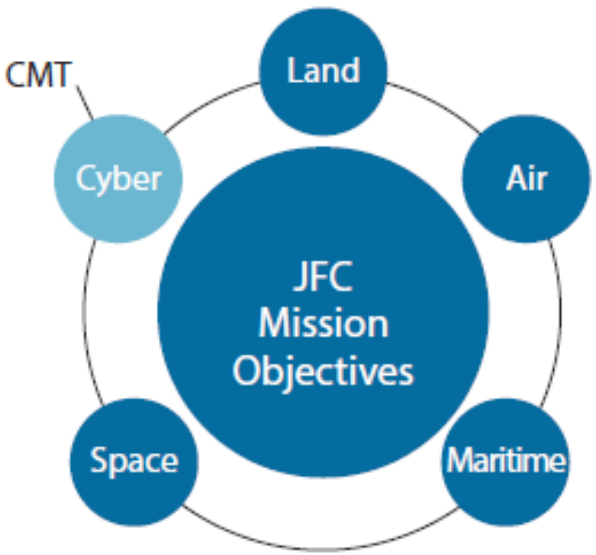
Cyber forces execute cyber actions:

Cyberspace Defense

Cyberspace OPE

Cyberspace ISR

Cyberspace Attack

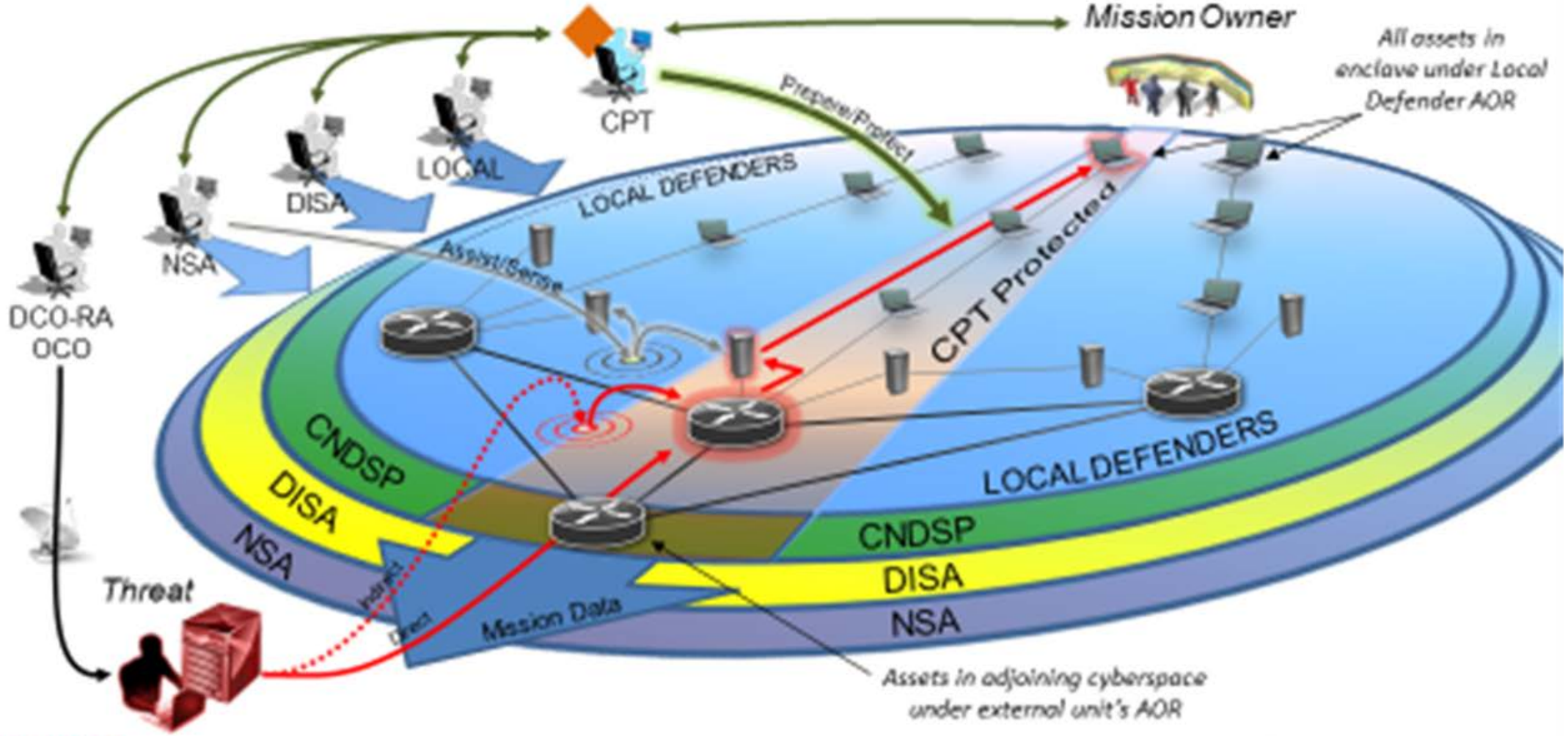


Supported by all-source intelligence, information technology, and routine communications activities

Defensive Cyber Operations (DCO)

- Mission Focused, Threat Specific, & Intelligence Driven
- Capabilities
  - Identify Key Terrain-Cyber (KT-C)
  - Discover, Detect, Analyze, & Mitigate Threats (includes insider threats)
- DCO-Internal Defensive Measures (IDM)
  - Hunt on friendly cyber terrain
  - “Stop the arrow” not the archer
- DCO-Responsive Actions (RA)
  - Reactive defense – “Stopping the shooter”
  - Mission of National Mission Teams under USCYBERCOM

CPT Area of Operation



CPT Employment

- CPTs execute three distinct missions (Survey, Secure, Protect)
  - Survey Mission -- Plan, Survey
  - Secure Mission -- Plan, Survey, Secure
  - Protect Mission -- All stages

- Each employment stage is dependent upon the previous one

- Each CPT squad has a unique role during each stage

Cyber Protection Teams (CPT)

CYBER LEADERSHIP
C2, Planning

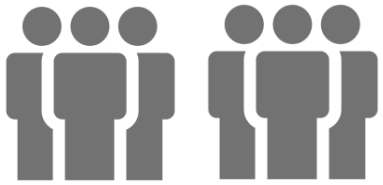
CPT Intelligence

Cyber Readiness (CR)	Cyber Support (CS)	Mission Protection (MP)	Defensive Cyber Infiltration (DCI)	Cyber Threat Emulation (CTE)
• Conducts compliance analysis • Provides detailed baseline evaluation • Coord/Conduct participative & non-participative Defense Evaluation (PDE/NPDE) • Recommendations to RMP & MDP • Ongoing monitoring • Assists in technical response actions	• Map Key Terrain-Cyber (TK-C) • Provides input to RMP • Assists in RMP implementation • Provides training to local defenders	• Lead for Id TK-C • Conducts comprehensive mission/risk analysis • Lead for Risk Mgt Plan (RMP) • Lead for MSN Defense Plan (MDP)	• Conducts recon to Id preexisting or active threats • Performs post exploitation forensics • Composes damage assessment • Assists in RMP & MDP • Supports PDE & NPDE	• Coordinate, collect, & share threat intelligence & TTPs • Instructs on threat TTPs • Conducts PDE and NPDE penetration testing • Emulates threats • Assists in RMP & MDP

Force Packages
By the Numbers

Scope

35



Mission-ready cyber professionals

Configuration

7

Member teams consisting of
1 Team Lead
1 Infrastructure Tech
1-2 Analysts
3-4 Cyber Operators

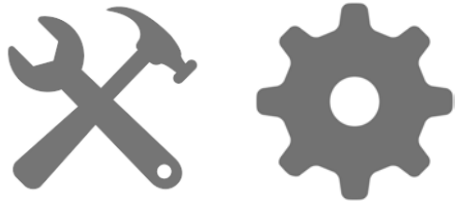
Employment

5 solo missions
2 formations

Can be either employed individually or as a coordinated multi-team package

Equipment

200+



Industry-standard tools are utilized by teams on standalone mission systems (local and remote capable)

Air National Guard
Cyber Protection Teams

- ***Federal**: Support the 24 AF operations with trained and ready cyberspace protection teams (CPT) to fill USCYBERCOM's Cyber Mission Force taskings*
- ***State of Iowa**: Ensure cyber preparedness and incident response for rapid internal state-level and national coordination needed to defend against cyber incidents across local, state and private industry partnerships*

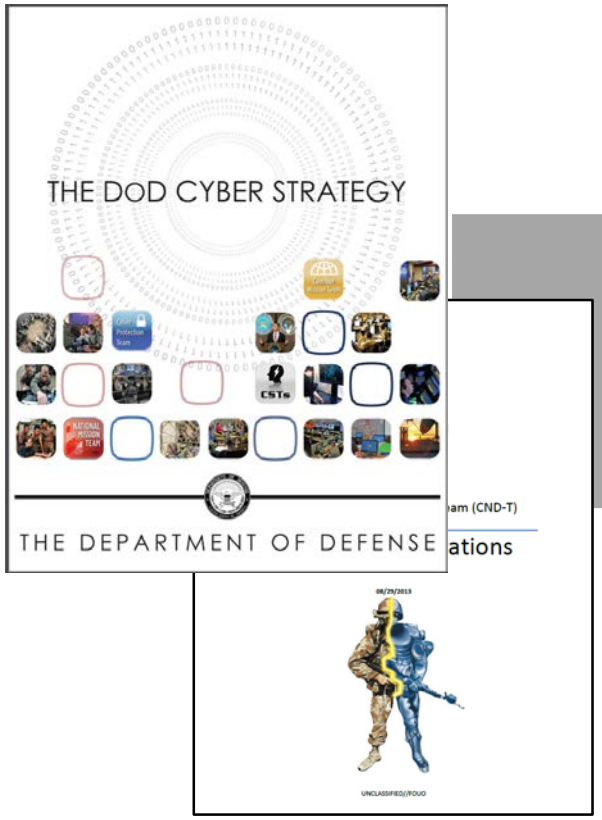
168th Cyber Operations Squadron
Force Packages for the State of Iowa

CYBER LEADERSHIP

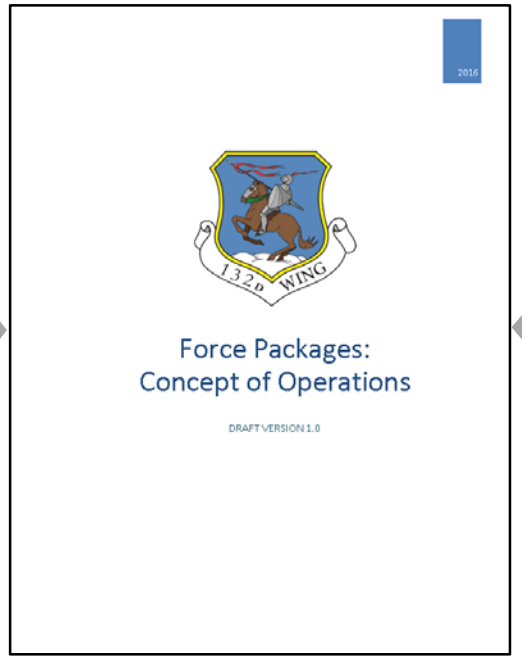
Authority for force planning, coordination, synchronization, and execution

SURVEY/ASSESS	PREVENT/RESPOND	INVESTIGATE/EMULATE	TRAIN/DEVELOP
Evaluates/sustains compliance and readiness	*Improves defense and augments response*	*Detects, illuminates, and emulates threats*	*Identifies, plans, and conducts training for local defenders*
• Conducts compliance analysis • Provides detailed baseline evaluation • Enhances/establishes compliance monitoring • Evaluates technical and risk mitigation measures; highlights shortfalls	• Conducts comprehensive mission/risk analysis • Performs vulnerability assessments • Enhances/implements mitigations • Augments incident response	• Identifies preexisting or active threats • Instructs on threat TTPs • Performs post exploitation forensics • Composes damage assessment • Conducts penetration testing and documents findings	• Reviews effectiveness of ops, policies, and procedures • Evaluates training needs and develops training plan • Performs immediate onsite training and recommends future formal instruction

Force Packages
Development Philosophy



Capabilities
Structure



Tasks
KSAs

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cyber Shield 2016
Background

- Two-week defensive cyber operations (DCO) training exercise
- Over 900 participants from state government agencies, federal agencies, industry partners, and academia
- 16 members from the 132d Cyber Operations Squadron (COS) participated in a variety of roles
  - Mission Protection (Blue Team)
  - Cyber Threat Emulation (Red Team)
  - Exercise Technical Analysis (White Team)
  - Intelligence Fusion Analysis
  - JAG Leadership

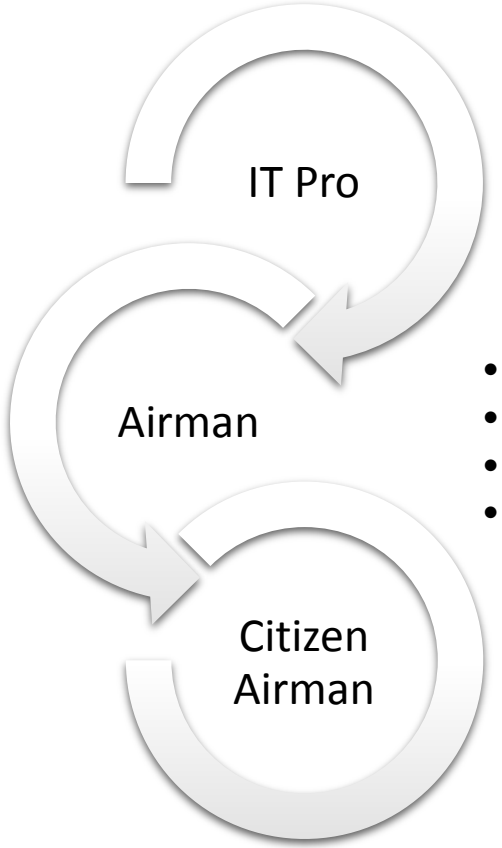
Cyber Shield 2016
Lessons Learned

- Relationships are critical; need for advance planning and partnering before incident arise
  - Industry Partner (i.e. acquaintance with our critical infrastructure industry partners systems in advance of a cyber event)
  - Agencies (FBI / Law Enforcement)
  - Legal (JAG)
  - Intel
  - Other states
- Ability to effectively adapt to uncertainties is crucial
  - Loss of network / range functionality
  - Loss of critical services (domain controller, web server, firewall, IDS/IPS)
  - Having to obtain supported partner's approval for network hardening requests
- Teams need a strong balance of technical skills and non-technical skills
  - Technical
    - Network Traffic Analysis
    - Windows / Linux Command Line
    - Network / Server / Host Administration
    - Cyber Incident Response
    - Malware Analysis
    - Triage /Incident Response Digital Forensics
  - Non-Technical
    - Teamwork
    - Composure
    - Communication
    - Indicators of Compromise and link analysis
    - Assertiveness, Leadership, & Followership
    - Ability to learn

Cyber Shield 2016
Legality

- Cyber Shield JAG Mission
  - To ensure the legality of our defensive cyber operations
  - Protect States/DoD/service members from liability
  - Integrate Judge Advocates (JA) with CPTs
  - Enhance partnerships with federal and state agencies involved in cyber operations
  - Maximize training for JAs and operators in domestic cyber operations and cyber law
- Cyber Law Key Tasks
  - Anticipate and identify potential legal issues; JAs prepared Cyber Shield legal resources guide
  - Train cyber teams to recognize cyber legal issues and engage JAG based on pre-approved actions
  - Embed JA with CPT to maximize JA training in Cyber operations; learn the area of operations
  - Draft documents to ensure successful coordination and understanding between the National Guard, the agency partner and interagency partners
- Iowa Air National Guard FY17-18 Cyber Law Next Steps
  - Cyber Operations Squadron (COS) Concept of Operations legal review
  - Cyber MOU/MOA's with Iowa State University and State of Iowa OCIO using the Iowa Communications Network, Minnesota Air National Guard (ANG)/Army Computer Network Defense Team, MidAmerican Energy, U.S. Air Force Academy Computer Science Department/Cyber Innovation Center
  - Iowa NG Cyber MOU and non-disclosure agreement template for future Cybersecurity support
  - Legal Review of Cyber Airmen Status to support T10 Missions

The Power of the Iowa Citizen Airman



- Technical Expertise
- Business Acumen
- Industry Leadership Skills

- Military Training & Expertise
- Military Leadership
- Dedication, Esprit de Corps
- Patriotism

- Well-rounded and Dynamic
- Technically Savvy
- Seasoned Longevity

LOCKHEED MARTIN

WELLS FARGO

General Mills

Wellmark BlueCross BlueShield

TRANSAMERICA

JOHN DEERE

DES MOINES POLICE

Rockwell Collins

IOWA DNR Natural Resources

132D WING

STATE

Booz | Allen | Hamilton

strategy and technology consultants

FARM BUREAU INSURANCE®

BOSCH

meredith

Questions