Army National Guard – Cyber Brigade

Colonel Adam Volant

AFCEA - Belvoir Industry Day

Overall Classification of this briefing is: UNCLASSIED//FOUO

TOPICS

- Definitions
- National Guard Cyber Formations
- ARNG Cyber Mobilizations
- Cyber Exercises
- ARNG EW Assets

What *IS* Cyber?

Presidential Commission

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY

Commission Final Report

- “The Guard represents a talent pool that can be regularly trained, equipped, and called on to protect and defend against attacks on information assets or computer systems and networks”
- Commission suggested that "state legislatures should give serious consideration to providing governors with the necessary authorities and resources to train and equip the National Guard to serve their states and safeguard the public from malicious cyber activity.”

Definition: Cyber Security

~~Provision or sustainment of **SERVICE**~~

Provision of **SECURITY**

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, **security** includes both cybersecurity and physical **security**.

Formation

91st Brigade colors unfurled October 2017

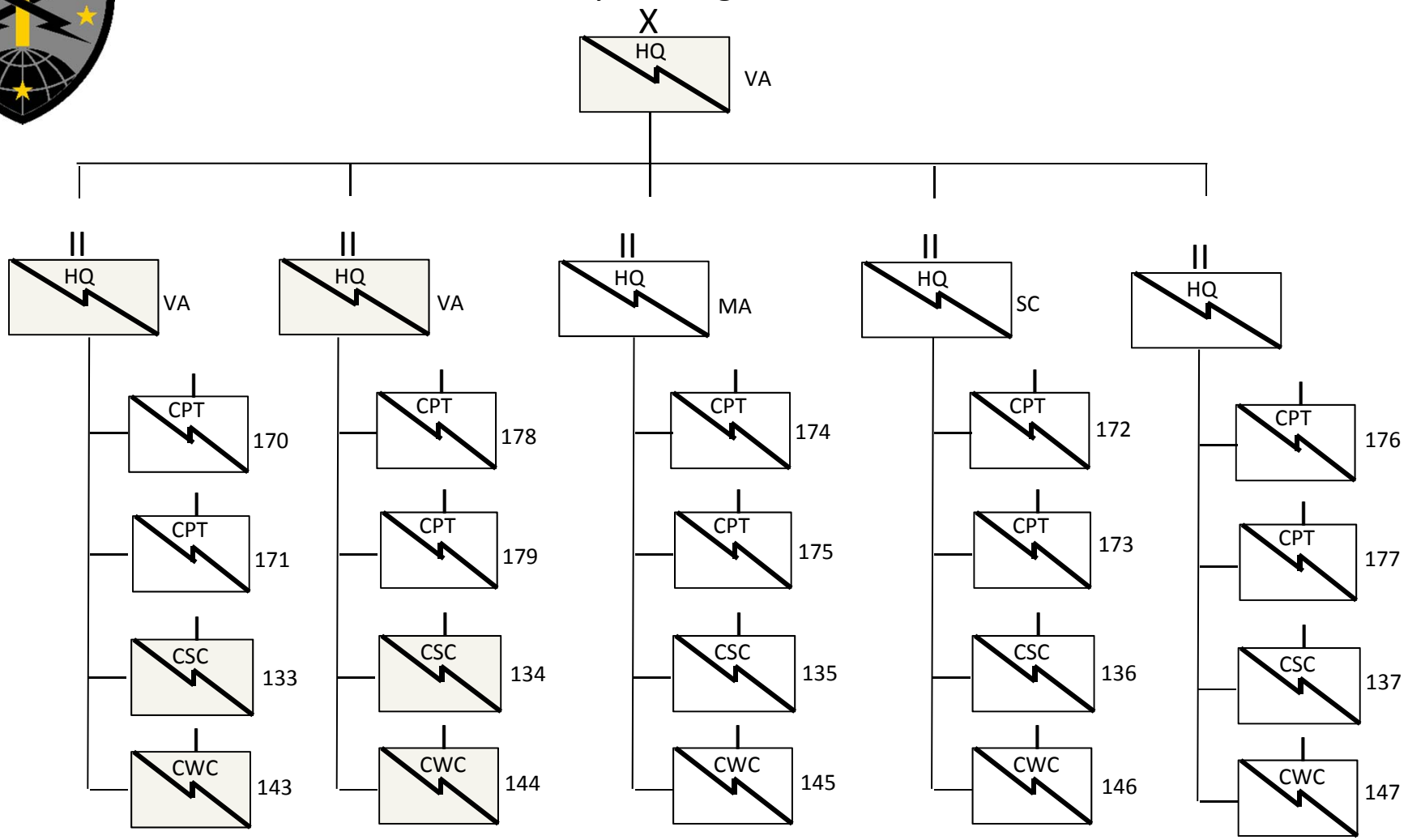
91st Cyber Brigade Patch

Five Stars for five battalions

One sword

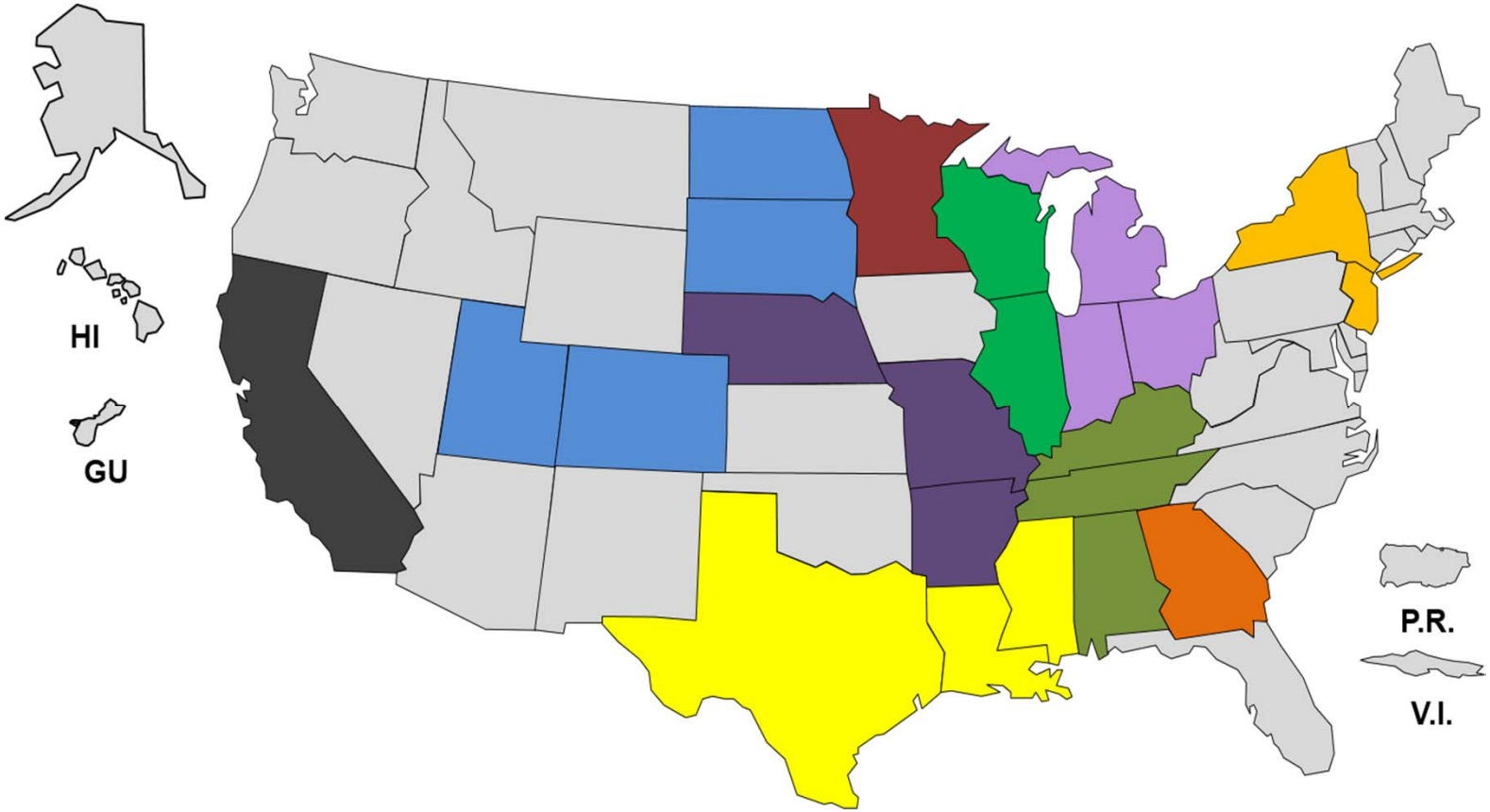
Two lightening bolts

91st Cyber Brigade



CPT: Cyber Protection Team (39 PAX)
CSC: Cyber Security Company (35 PAX)
CWC: Cyber Warfare Company (32 PAX)

New ARNG CPT Units

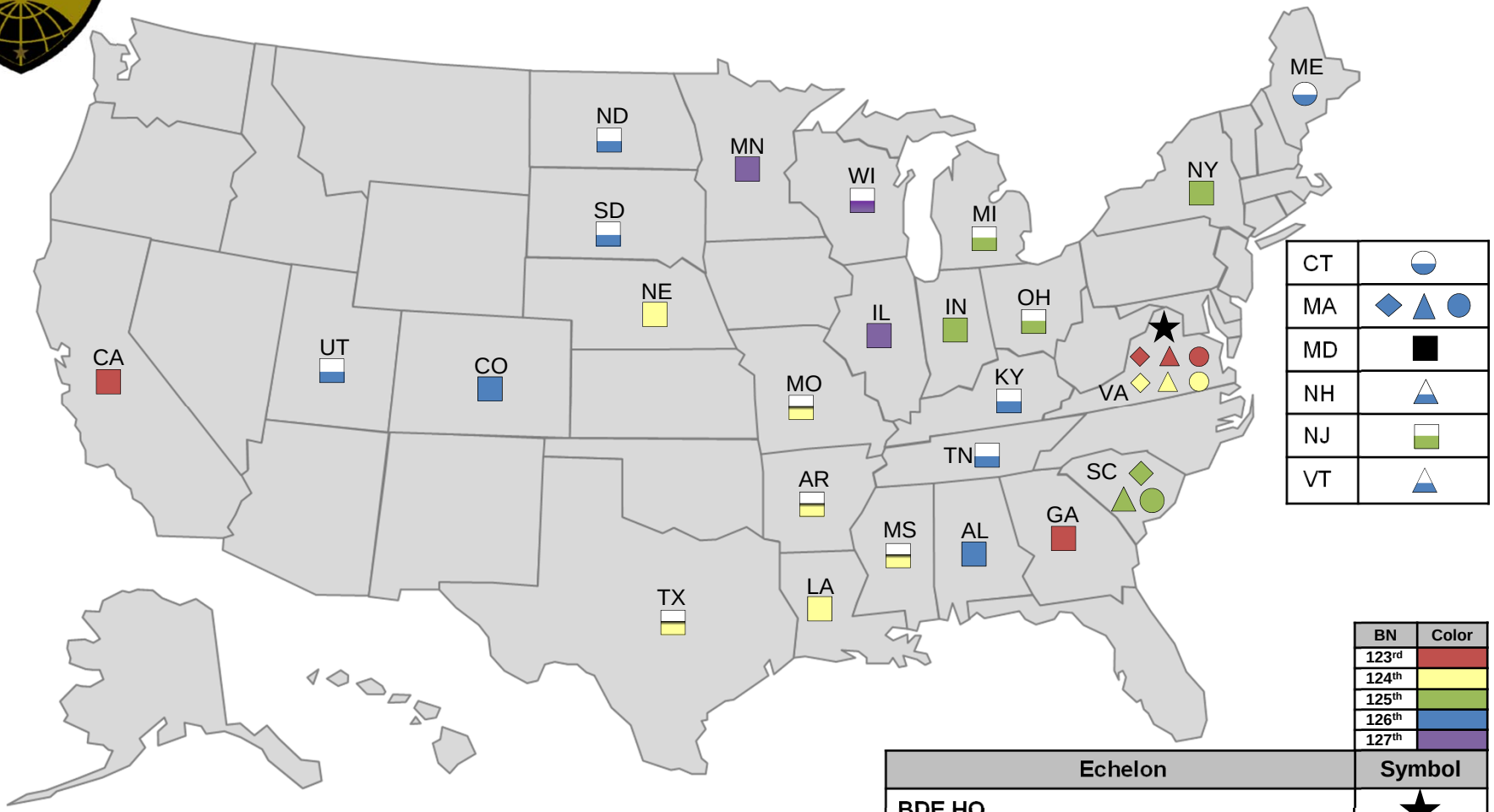


FY17 Teams (stand up in FY16)
- CPT 170
- CPT 171
- CPT 172

FY18 Teams (stand up in FY17)
- CPT 173
- CPT 174
- CPT 175
- CPT 176

FY19 Teams (stand up in FY18)
- CPT 177
- CPT 178
- CPT 179

91st Cyber Brigade



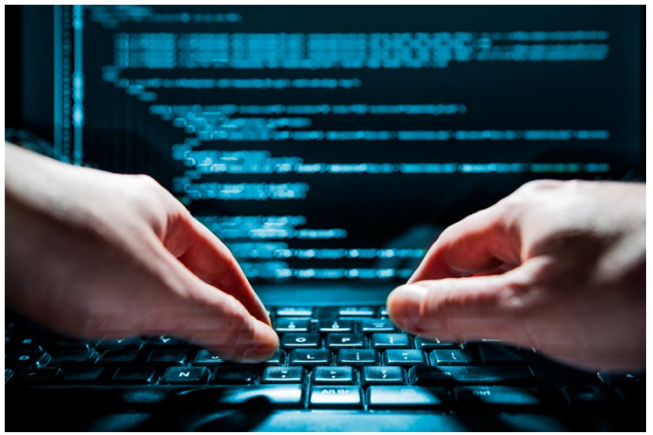
BN	Color
123rd	
124th	
125th	
126th	
127th	

Echelon	Symbol
BDE HQ	★
BN HQ	◆
Cyber Security Company (CSC) HQ / Det	▲ ◬
Cyber Warfare Company (CWC) HQ / Det	● ◓
Cyber Protection Team (CPT) HQ / Det	■ ◪

Cyber Security Company

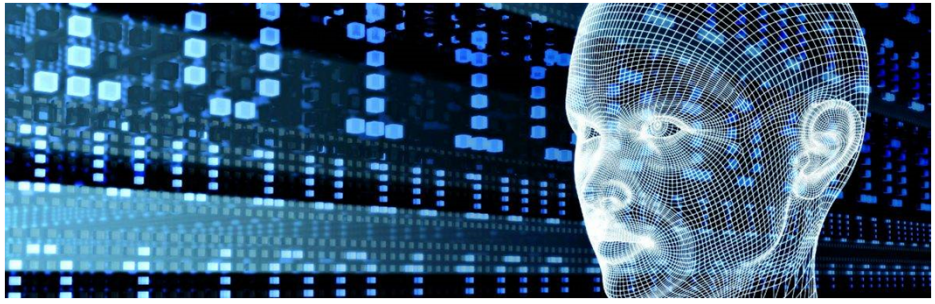
Conduct Defensive Cyberspace Operations (DCO) in support of Corps and below, other unified land operations, and the Joint Force, which includes Cyber Command readiness inspections, **Vulnerability Assessments**, **forensics analysis, critical infrastructure assessment** and support, and Cybersecurity support. Provide Mission Command to Cyber Security Team, Cyber Security Support Team, and Critical Infrastructure Team which includes operational direction and guidance in the conduct of Defensive Cyberspace Operations.

.



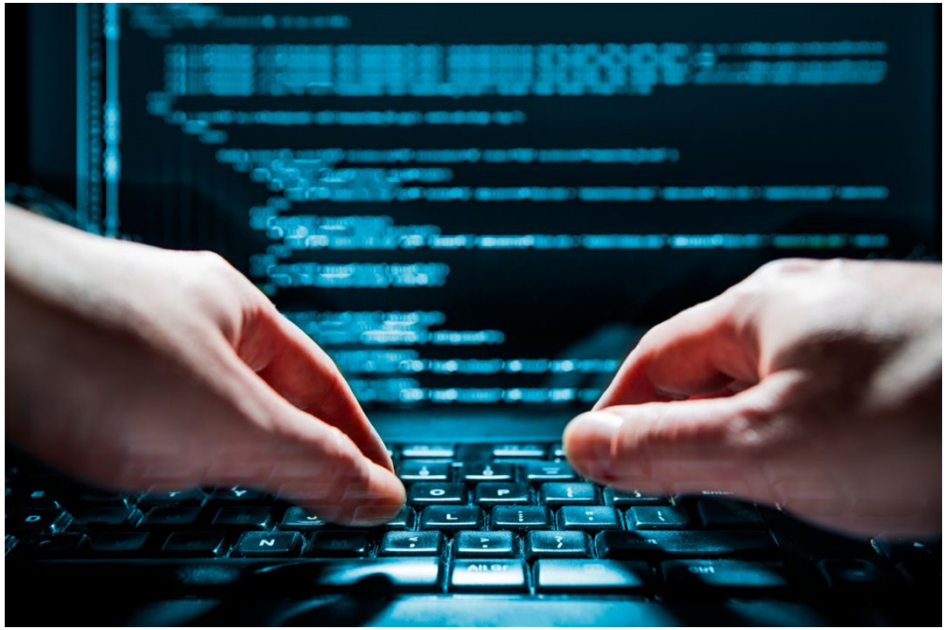
Cyber Warfare Company

Conduct Defensive Cyberspace Operations (DCO) in support of Corps and below, other Unified Land Operations, and the Joint Force, which includes **Cyber OPFOR support, Network Warfare activities, and Cyberspace Operational Preparation of the Environment (OPE) actions**. Provide Mission Command and operational support to the Network Warfare Team, Cyber Analysis Team, and the Cyber Support Team, which includes orders and guidance in the execution of Cyberspace Operations.



Cyber Protection Team

Conduct Defensive Cyberspace Operations (DCO) on military networks to support mission requirements. In compliance with federal and state laws, DCO may be expanded to include Cyber Command Readiness Inspections, **Vulnerability Assessments, Cyber OPFOR support, Critical Infrastructure Assessments, support for Theater Security Cooperation activities, Training support, and Advisory and Assistance support**.



Army Cyber Training

CYBER COMMON TECHNICAL CORE

- **Overview**
  A nine-week course focused on the development of a Cyber Soldier's technical foundation. This course is taught at an intermediate level, and is split into four modules: *Windows, Linux, networking and security*. Each module lasts two weeks.
- **What You'll Learn**
  Small-unit tactics, technical cyberspace operations training, Army operations intelligence, military decision making process, offensive and defensive cyberspace operations

Army Cyber Training

ADVANCED CYBER OPERATIONS SPECIALIST

- **Overview**
  Cyber Operations Specialist is a 20-week course, and serves as the foundation for your skills in the Cyber Operations Specialist (17C) MOS.
- **What You'll Learn**
  Warrior tasks and battle drills, *computer programming in the languages of Python and C*. In addition, students will learn common technical core skills in cyberspace operations, and core methodologies to lead cyber protection teams. Finally, students will learn to analyze offensive cyberspace operations tactics.

Industry Relevant Training

Task Force ECHO Mission

Members of the Army National Guard from California, Georgia, Indiana, Ohio, Michigan, Virginia and Utah will be mobilized to engineer, install, operate and maintain a critical infrastructure for US CYBERCOM.

Task Force ECHO Magazine Cover

Article: “Fortifying Our Cyber Defense”

CW2 William Bayse

- 6+ years DoD Civilian, leading various teams of Cyber Forensics Analysts in support of defensive cyber operations.
- 8+ years DoD Contractor, providing cyber security, information assurance, and systems & network administration services.

- 19+ years total service, including Active Duty and National Guard.
- Most recent assignments: Cyber Ops Tech, SASMO, Battalion Deputy S6.
- Supported two Presidential Inaugurations and more than five State Active Duty (SAD) Emergency Support missions.

Kodiak Cyber Operations Team

Direct IO, EW and Cyber Support to the Warfighter

- Predates creation of ARCYBER
- Draws from ARNG Cyber Brigade
- Currently filled with SC Cyber Warfare Company

KCOT

KCOT

Mission

To support Combatant Commanders and Joint Task Forces global requirements, by conducting Information Operations, Electronic Warfare, Offensive Capabilities and supporting the fielding and operationalization of new capabilities, in an immediate and timely operational response.

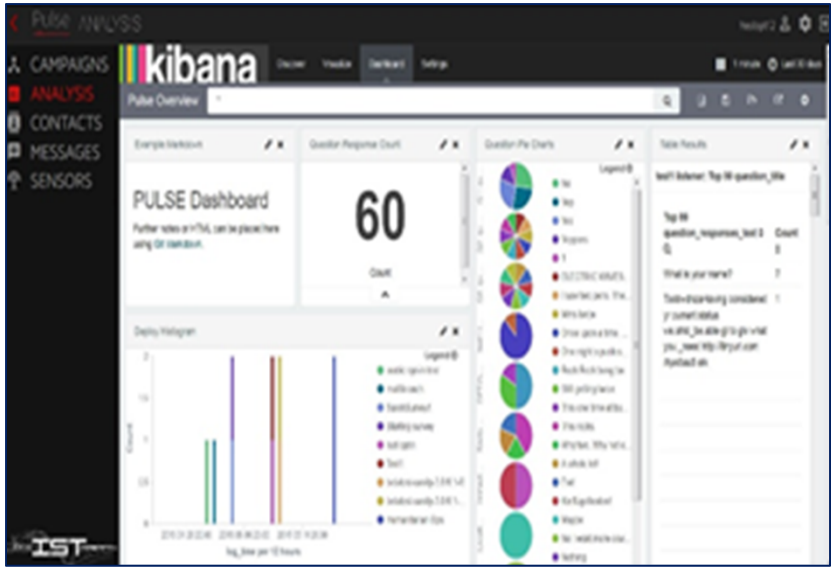
Tasks

- Deliver IO, MISO and MILDEC content via web pages, SMS/MMS, and e-mail.
- Provide SMEs to planning efforts, capability development, and R&E.
- Provide technical expertise towards the development process, testing, staging, standardizations and incorporations into established planning and targeting processes.

KCOT

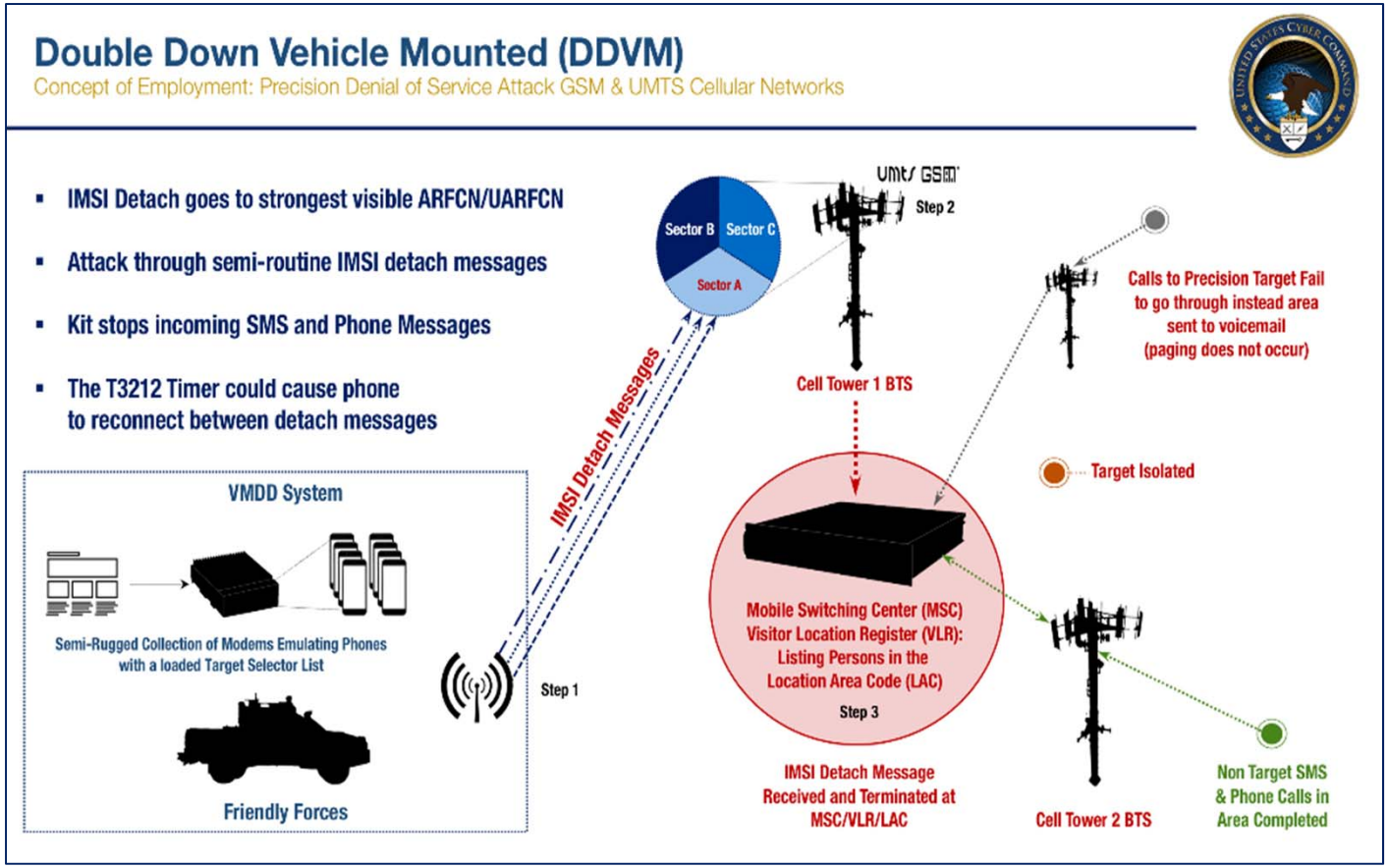
PULSE

- Integrates technology and methodology to enable rapid, dynamic, mission-focused engagement to cellular networks
- rapidly configures a system for two-way communication across numerous channels (e.g., Short Message System (SMS), Multi-media Message System (MMS), Interactive Voice Response (IVR)



KCOT

DDVM



Double Down Vehicle/Rack Mount (DDVM/DDRM) are custom and modified commercial hardware solutions that supports network scanning, surveying, area and precision Denial of Service (DoS) attacks against GSM, UMTS and LTE cellular networks.

KCOT

Web Hosting

- KCOT supports the creation, provisioning, and updating of Web Hosting capabilities per individual mission requirements.
- Web Hosting in EC2 is a basic method of placing up phishing sites, information operations and other deception campaigns critical to penetration testing

Mission Objective: Delivery IO content to Arabic.rt.com users.

Delivered to:

- Main Page, left most picture link:
- Business Section link
- Web Page in Business Section

Title:

لقاء قريب الجوي بين الولايات المتحدة والطائرات السورية

Author:

أحمد الموح

Main Text:

مقاتلتين من ميل داخل طار ،سوريا ،الحسكة على دورية في F-22S الأمريكية التين ان ان سي الامريكية الدفاع وزارة في مسؤول وقال
الجمعة بمغادرة لهم "تسجح" و السورية 24-سو.
قوات اضطر مما ،المتحدة للولايات رئيسي حليف وهو ،للأكراد السورية حربيتان طائرتان هاجمت أن بعد فقط واحد يوم قريب لقاء ويأتي
.سوريا شمال في مركزها من تسحب أن إلى الأمريكية الخاصة العمليات

هجوم بعد أعلن قد البنتاغون كان التي المنطقة في لبنان في الموقتة المتحدة الولايات الجوي القتال دوريات من جزء هي الأمريكية الطائرات
.الخميس يوم
على حصلت ولكن القيادة قمرة إلى القيادة قمرة السورية الطائرات لاستدعاء رابتورز F-22 من الطيارين حاول أمريكي مسؤول وأضاف
.رد أي
سوريا موقف من الأمريكية الخاصة العمليات قوات انسحبت قد الجيش أن سابق وقت في CNN الامريكية الدفاع بوزارة مسؤولون وقال
.الحسكة من وحولها المدينة في كردية مواقع مهاجمة ،قريب قصف السوري الجيش بدأ أن بعد بهم شمال
شمال في ،وجدت إن ،تتراك عدد الفور على يتضح ولم ،مواقعها من انتقلت التي الأمريكية القوات من نسبيا قليل عدد كان المسؤول وأشار
.سوريا
.لمسؤولين وفقا ،السوري القصف خلال المتحدة الولايات قوات أي أصيب
."طائرة فقدان من كبير خطر في هم ،أخرى مرة هذا السوريون حاول إذا" :CNN اخر كبير دفاعي مسؤول وقال
لعدة المنطقة في الأمريكية الخاصة العمليات قوات وكانت .البنتاغون في مسؤولون استقرار وزعزع الحسكة منطقة في وقع الذي الهجوم
الولايات الرئيسي الحليف ،السورية الديمقراطية والقوى والكردية العربية العناصر مع الاستشارية والبعثات التدريب إجراء أشهر (SDF)
.المنطقة في المتحدة
،استجابة هناك يكن لم ولكن ،مشتركة إذاعية قناة على السورية الطائرات لاستدعاء الأرض على التحالف قوات وحاولت ،القصف بدأ عندما
.ديفيس جيف الكابتن البنتاغون باسم للمتحدث وفقا
سابقا المحددة قناة على الروس بسرعة دعا المتحدة الولايات موظفي ولكن .السوريين إلى للوصول التحالف قوات حاولت ما القول ورفض
واضحة النقطة هذه في المتحدة الولايات قدمت .لها يكن لم المتحدة الولايات في الروس أكد ديفيس وقال .يطلق الذي من لمعرفة محاولة في
.الضربات استمرت اذا الأرض على الامريكية القوات عن للدفاع "الضرورية الاجراءات كل ستتخذ" المتحدة الولايات أن الروس خلال من

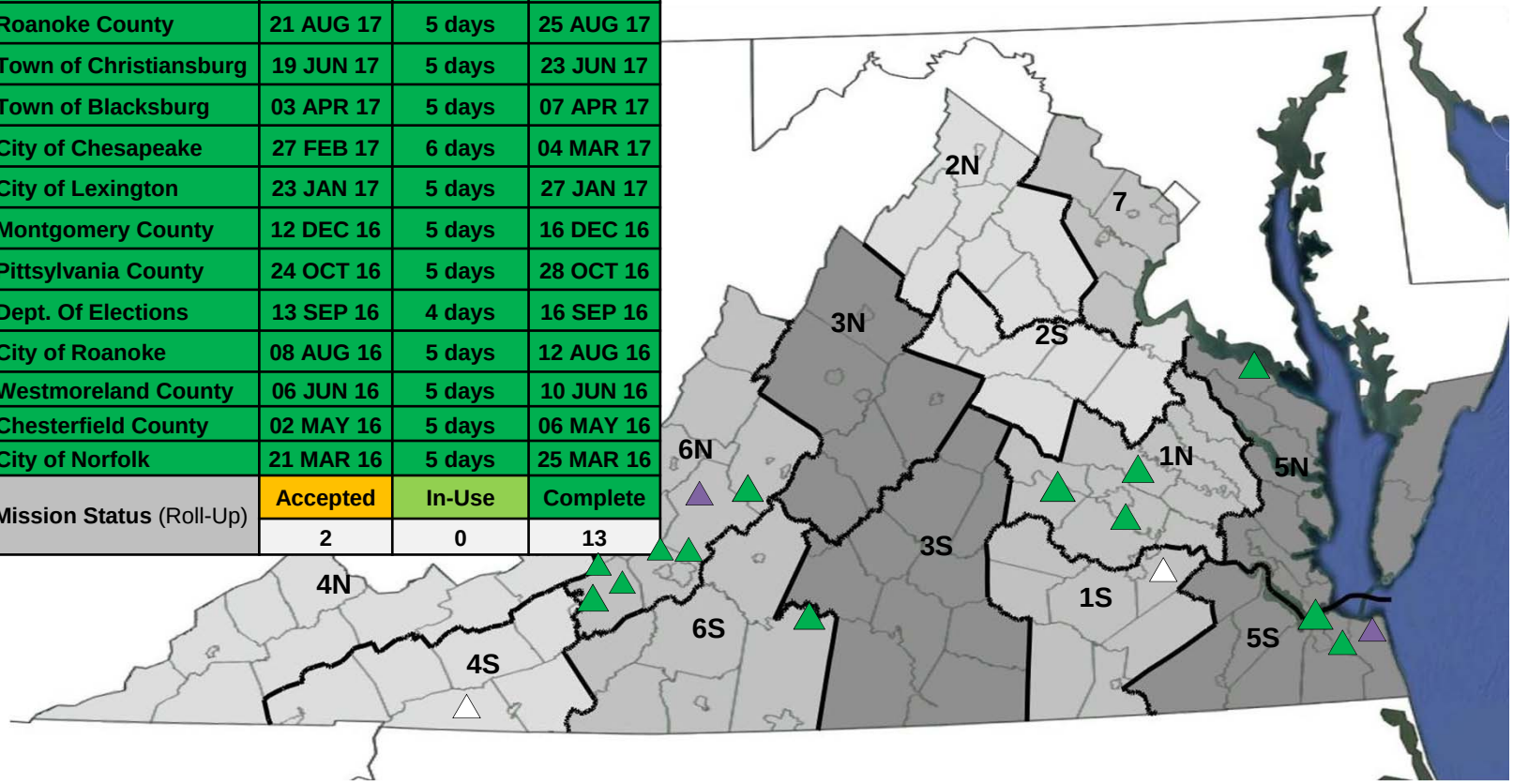
State Cyber Support Mission Summary

As of 050800RDEC2017

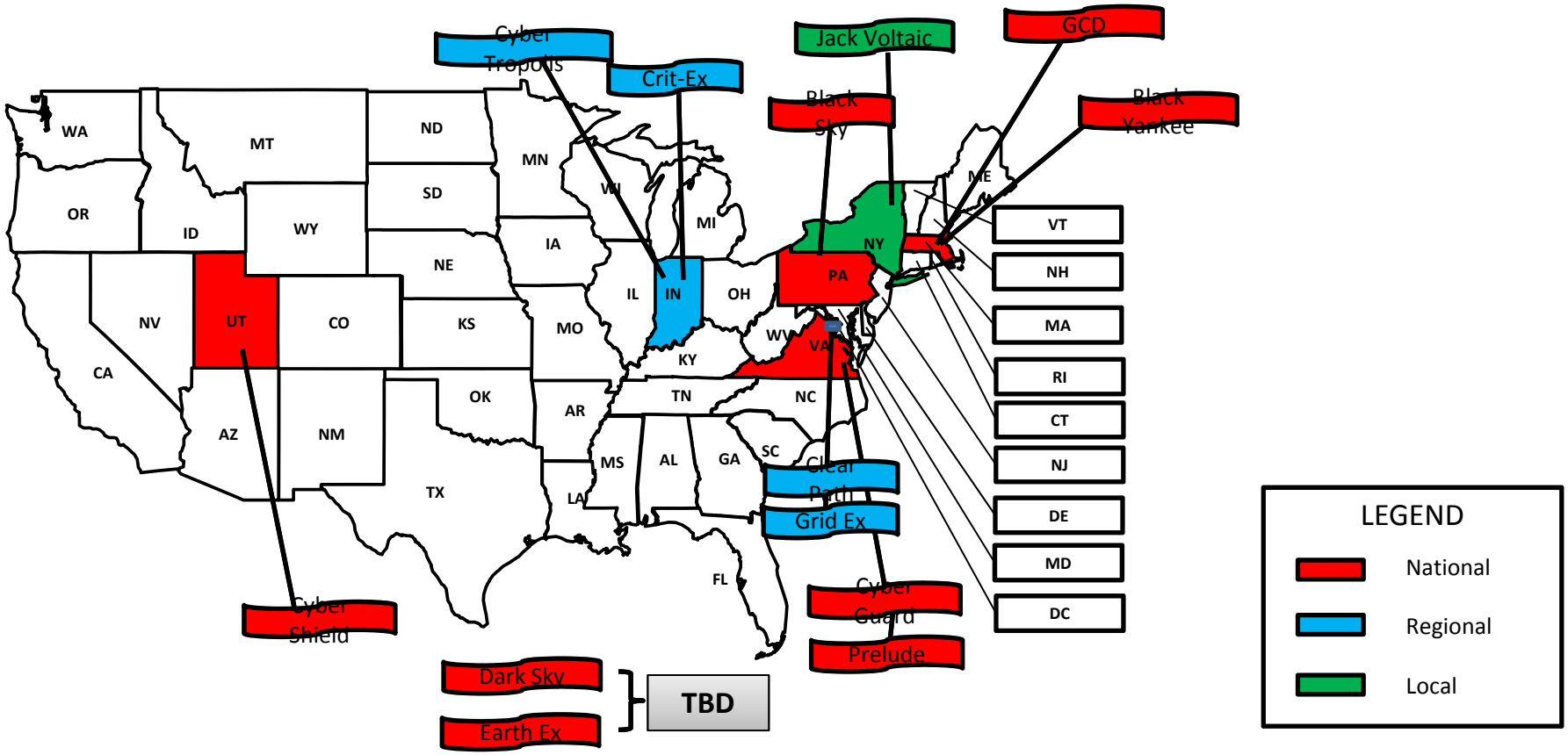
Mission #	PAX	Mission Location (Locality/Agency)	Mission Start Date	Mission Duration	Mission End Date
	TBD	Prince George County	MAR 18	5 days	TBD
	TBD	Washington County	APR 18	5 days	TBD
17-0503-05	TBD	Virginia Beach Schools	JAN 18	5 days	JAN 18
17-0424-10	TBD	Botetourt County	FEB 18	5 days	FEB 18
17-0424-08	4	Powhatan County	18 SEP 17	5 days	22 SEP 17
17-0424-09	5	Roanoke County	21 AUG 17	5 days	25 AUG 17
17-0424-07	6	Town of Christiansburg	19 JUN 17	5 days	23 JUN 17
17-0424-06	4	Town of Blacksburg	03 APR 17	5 days	07 APR 17
17-0424-05	4	City of Chesapeake	27 FEB 17	6 days	04 MAR 17
17-0424-04	5	City of Lexington	23 JAN 17	5 days	27 JAN 17
17-0424-03	5	Montgomery County	12 DEC 16	5 days	16 DEC 16
17-0424-02	5	Pittsylvania County	24 OCT 16	5 days	28 OCT 16
16-0424-00	5	Dept. Of Elections	13 SEP 16	4 days	16 SEP 16
16-0424-01	6	City of Roanoke	08 AUG 16	5 days	12 AUG 16
16-3595-03	5	Westmoreland County	06 JUN 16	5 days	10 JUN 16
16-2957-02	6	Chesterfield County	02 MAY 16	5 days	06 MAY 16
16-2946-01	6	City of Norfolk	21 MAR 16	5 days	25 MAR 16
Total PAX (To Date)	66	**Mission Status** (Roll-Up)	Accepted	In-Use	Complete
			2	0	13

ISSUES / CONCERNS

- Engaged with Washington County – APR 2018 (tentative)
- Engaged with Prince George County – MAR 2018 (tentative)
- Accepted Botetourt County mission – FEB 2018
- Accepted Virginia Beach Schools mission – JAN 2018



Cyber Exercise Locations



Cyber Yankee Overview

Classification: Unclassified

The goal of Cyber Yankee is to create a realistic cyber exercise for Army National Guard Cyber Network Defense Teams (CNDT) to further train and apply their skills as cyber defenders. The exercise focuses on developing strong collaboration across all of the New England Cyber and Intel teams/units. The **emphasis is on learning key skills in cyber defense and reporting within an Inter-service and Inter-agency operational environment**. Our end state is the development of a more robust collection of cyber teams within our region along with a growth in partnerships across multiple levels of government.

Cyber Shield Overview

Classification: Unclassified

To **collectively train and validate Army National Guard Defensive Cyberspace Operations Elements (DCO-E) Internal Defensive Measures (DCO-IDM) and the National Guard Coordinate, Train, Advise, Assist (CTAA) Mission**. Cyber Shield 2018 is a National Guard Bureau exercise that achieves unity of effort with and between ARNG DCO-E, National Guard and U.S. Army Reserve Cyber Protection Teams, and Mission Partners to achieve mission success.

Cyber Guard Overview

Classification: Secret

Cyber Guard 18 (CG18) will be at the operational level and geographically dispersed. CG18 will **explore resource constraints, requests for assistance, command and control and Defense Support to Civilian Authorities**. CG18 participants will operate from their home stations and exercise with stakeholders and peers from across the county.

Jack Voltaic Overview

Classification: Unclassified

Led by the Army Cyber Institute at West Point in partnership with AECOM, Jack Voltaic 2.0 is an innovative **public-private exercise designed to help cities assess and prepare for a complex cyber-attack**. By simulating a combined physical and cyber-attack impacting multiple critical infrastructure sectors, Jack Voltaic 2.0 assesses the host city's ability to respond and examines the integration of the National Guard's cyber incident response. Jack Voltaic 2.0 builds on the inaugural Jack Voltaic exercise held in 2016. The Army Cyber Institute will use the results of Jack Voltaic 2.0 as a preparation frame-work for municipalities throughout the U.S. This experiment will improve the host city's incident response capabilities and identify gaps not addressed by other exercises.

ARNG Electronic Warfare

- ARNG is poised to support proposed EW force design for BCT & EMIB formations, and corps and below capability development.
- 901 billets for EW trained officer and enlisted

Are there hints to the future?

Disruption is normal

COL Adam C. Volant | 540-570-1839
adam.c.volant.mil@mail.mil

Exercise Descriptions

Black Sky – An exercise intended to prepare government agencies, utility commissions, military, and law enforcement agencies, and emergency responders for response plans in the event of a large scale, hazardous incident.

Clear Path – Exercised focused on strategic level response operations and the coordination between government and industry.

Crit-Ex – Exercise discussion-based of response to a cyber attack on an electrical power plant, which generates cascading effects into the water/wastewater sector.

Cyber Guard – Exercise consisting of whole nation response to destructive cyber attack against the U.S. critical infrastructure. Designed to defend DoDIN and mitigate damage to critical infrastructure in a compromised cyber environment.

Cyber Guard Prelude – About exercising information sharing mechanisms, resource allocation, and augmentation processes, and other plans and procedures during a widespread series of cyber incidents.

Cyber Shield – Culminating training event that supports the NG's defensive cyberspace operations missions to defend the Department of Defense assets by conducting cyber command readiness inspections and critical infrastructure vulnerability assessments.

Cyber Tropolis – Team Validation event; One team on business network and the other on the operational network.

Cyber Yankee – Joint tactical level cyber exercise bringing together US Army NG, DJS, FEMA, FBI, and USSS.

Dark Sky – An exercise series to conduct red team assessments before an exercise and then notionally re-create traffic on a network to play out incident response and escalation procedures.

Earth-Ex – An Emergency all sector response transnational hazard exercise to evaluate improve restoration support, preparedness, response, and recovery plans for severe hazards.

GCD – Establish training objectives, discuss ideas for increased realism or greater challenge, identify/prioritize new tools that should be virtualized, and shape the structure for the exercise in coming years.

Grid Ex – 2 year planning cycle, national level, unclassified, public-private exercise designated to simulate a coordinated cyber/physical attack with operational impacts on electric and other critical infrastructure across North America to improve security, resiliency, and reliability

Jack Voltaic – Exercise with scope and objectives to demonstrate a cyber attack focused within a municipality, impacting multiple sectors and to exercise a city's ability to respond to an attack

Cyber Battalion Initial Operational Capability

IOC Battalion Breakdown	
Battalion	10 of 26
Cyber Warfare	12 of 33
Cyber Security	15 of 36
Total	37 of 95

Within the positions reflected Soldiers will be MOSQ'd and/or in the position based off of work roll experience

BATTALION			CYBER WAREFARE COMPANY			CYBER SECURITY COMPANY		
BN COMMANDER	05	17A00	CO COMMANDER	04	17A00	CO COMMANDER	04	17A00
CO COMMANDER	03	01A00	CYBER OPS TECH	02	17A00	TEAM LEADER	03	17A00
SUPV SUPPLY NCO	E7	92Y10	CYBER OPS NCO	E6	17C30	INFO SYS OFF	02	25A00
SUPV HUMAN RESOURCE NCO	E7	42A40	CYBER OPS SGT	E5	17C20	SR CYBER NET DEFENDER	E6	25D30
ALL SOURCE INTEL TECH	W4	350F0	ALL SOURCE INTEL TECH	W4	350F0	SR ALL SOURCE INTEL ANAL	E6	35F30
CYBER OPS PLANNER	03	17A00	SR CRYPT NET WAR NCO	E7	35Q40	CYBER NET DEFENDER	E5	25B20
SUPV CYBER OPS NCO	E7	17C40	CRYPT NET WAR NCO	E6	35Q30	NETWAR OFF	W4	255S0
SR CYBER NETWORK DEF NCO	E6	25D30	CRYPT NET WAR SPEC	E4	35Q10	INFO SYS OFF	02	25A00
SR SUPPLY SGT	E6	92Y30	CYBER SEC TECH	W4	255S0	SR CYBER NET DEF	E6	25D30
S6	03	25A00	INTERACTIVE OPERATOR	E6	35Q30	INFO SYS MANAGER	E5	25B20
			SR INFO TECH NCO	E6	25D30	INFO SYS MANAGER	E5	25B20
			ALL SOURCE INTEL ANAL	E5	35F20	TEAM LEADER	03	17A00
						CYBER OPS SUPV	E7	17C40
						CYBER OPS NCO	E6	17C30
						CYBER OPS SGT	E5	17C20

Cyber Battalion Fully Operational Capability

Battalion Breakdown	
Battalion	22 of 26
Cyber Warfare	28 of 33
Cyber Security	31 of 36
Total	81 of 95

Within the positions reflected Soldiers will be MOSQ'd and/or in the position based off of work roll experience

BATTALION			CYBER WAREFARE COMPANY			CYBER SECURITY COMPANY		
BN COMMANDER	05	17A00	CO COMMANDER	04	17A00	CO COMMANDER	04	17A00
CO COMMANDER	03	01A00	CYBER OPS TECH	02	17A00	TEAM LEADER	03	17A00
SUPV SUPPLY NCO	E7	92Y10	CYBER OPS NCO	E6	17C30	INFO SYS OFF	02	25A00
SUPV HUMAN RESOURCE NCO	E7	42A40	CYBER OPS SGT	E5	17C20	SR CYBER NET DEFENDER	E6	25D30
ALL SOURCE INTEL TECH	W4	350F0	ALL SOURCE INTEL TECH	W4	350F0	SR ALL SOURCE INTEL ANAL	E6	35F30
CYBER OPS PLANNER	03	17A00	SR CRYPT NET WAR NCO	E7	35Q40	CYBER NET DEFENDER	E5	25B20
SUPV CYBER OPS NCO	E7	17C40	CRYPT NET WAR NCO	E6	35Q30	NETWAR OFF	W4	255S0
SR CYBER NETWORK DEF NCO	E6	25D30	CRYPT NET WAR SPEC	E4	35Q10	INFO SYS OFF	02	25A00
SR SUPPLY SGT	E6	92Y30	CYBER SEC TECH	W4	255S0	SR CYBER NET DEF	E6	25D30
S6	03	25A00	INTERACTIVE OPERATOR	E6	35Q30	INFO SYS MANAGER	E5	25B20
BN XO	04	17A00	SR INFO TECH NCO	E6	25D30	INFO SYS MANAGER	E5	25B20
CSM	E9	00Z60	ALL SOURCE INTEL ANAL	E5	35F20	TEAM LEADER	03	17A00
FIRST SERGEANT	E8	00F50	COMPANY XO	03	17A00	CYBER OPS SUPV	E7	17C40
S1	03	42H00	FIRST SERGEANT	E8	00F50	CYBER OPS NCO	E6	17C30
SR HUMAN RESOURCE NCO	E6	42A30	TEAM LEADER	03	17A00	CYBER OPS SGT	E5	17C20
S2	03	35D00	CYBER OPS TECH	W4	170A0	COMPANY XO	03	17A00
SUPV INTEL NCO	E7	35F40	CYBER OPS SUPV	E7	17C40	FIRST SERGEANT	E8	00F50
S3	04	17A00	CYBER OPS SGT	E5	17C20	CYBER OPS TECH	W4	170A0
CYBER OPS TECH	CW4	170A0	TEAM LEADER	03	17A00	SUPV CYBER NET DEF	E7	25D40
SR CYBER OPS NCO	E6	17C30	CYBER OPS TECH	W4	170A	SR CYBER NET DEFENDER	E6	25D30
S4	03	90A00	CYBER OPS TECH	02	17A00	ALL SOURCE INTEL ANAL	E5	35F20
SR INFO TECH NCO	E6	25B30	CRYPT NETWAR NCO	E6	35Q30	TEAM LEADER	03	25A00
			ALL SOURCE INTEL ANAL	E4	35F10	ALL SOURCE INTEL TECH	W4	350F0
			TEAM LEADER	03	25A00	SUPV CYBER NET DEF	E6	25D40
			NETWORK ENGINEER	02	25A00	SR CYBER NET DEF	E6	25D30
			SUPV INTEL SPC	E7	35F40	INFO SYS MANAGER	E5	25B20
			SR INFO TECH NCO	E6	25D30	INFO SYS TECH	E4	25B10
			INTERACTIVE OPERATOR	E5	35Q20	CYBER OPS TECH	W4	170A0
						CYBER OPS TECH	02	170A00
						CYBER OPS NCO	E6	17C30
						CYBER OPS SPEC	E4	17C10