U.S. Army Cyber Center of Excellence and Fort Gordon

WHERE TRADITION MEETS THE FUTURE
Team Gordon
UNITED STATES ARMY
CYBER
CENTER OF EXCELLENCE · FORT GORDON

BUILDING A WORLD CLASS CYBER WORKFORCE

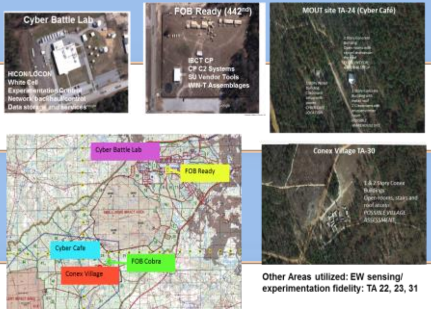
Cyber Quest 2018

21 Aug 2018

Cyber Quest:

Enabling CEMA Operations Within a Multi-Domain Battle

A world-class, Army led, **prototype assessment** conducted in an **operationally relevant environment** with government, industry and academia partners to identify **innovative** Intel, Signal, Cyberspace, and Electronic Warfare technologies.



Other Areas utilized: EW sensing/ experimentation fidelity: TA 22, 23, 31

Prototype Assessment

- Validate/inform concept development
- Inform requirements generation
- Identify candidate technologies for JWA/NIE
- Quick-turn integration of mature capabilities

Environment

- Focused at BDE (IBCT) and below
- Focused on AWfC #1, #7, #19
- Live, Constructive, Virtual Environment

Innovation

- Vendor solution coupled with current baseline
- Direct operator feedback from Soldiers
- No fear of failure – Sandbox strategy

CQ 2016 Highlights

- *CEMA Construct*
- *EW/Cyber Situational Awareness*
- *Soldier as a Sensor*
- *MFEW Concepts & Learning Demands*
- *Big Data & Data Analytics*

CQ 2017 Focus

- *Improve tactical communications capacity, reach & security*
- *DCO Mission visualization, planning & management*
- *EW Mission visualization, planning & management*
- *Situational Understanding*

Pre-Decisional

CQ 2018/2019/2020 Themes

- *2018:* Cyberspace Electromagnetic Activities (CEMA) enabling the Multi Domain Battle
- *2019:* Joint interoperability for next generation warfare
- *2020:* Retaining Cyberspace Key Terrain during Multi-Domain Battle

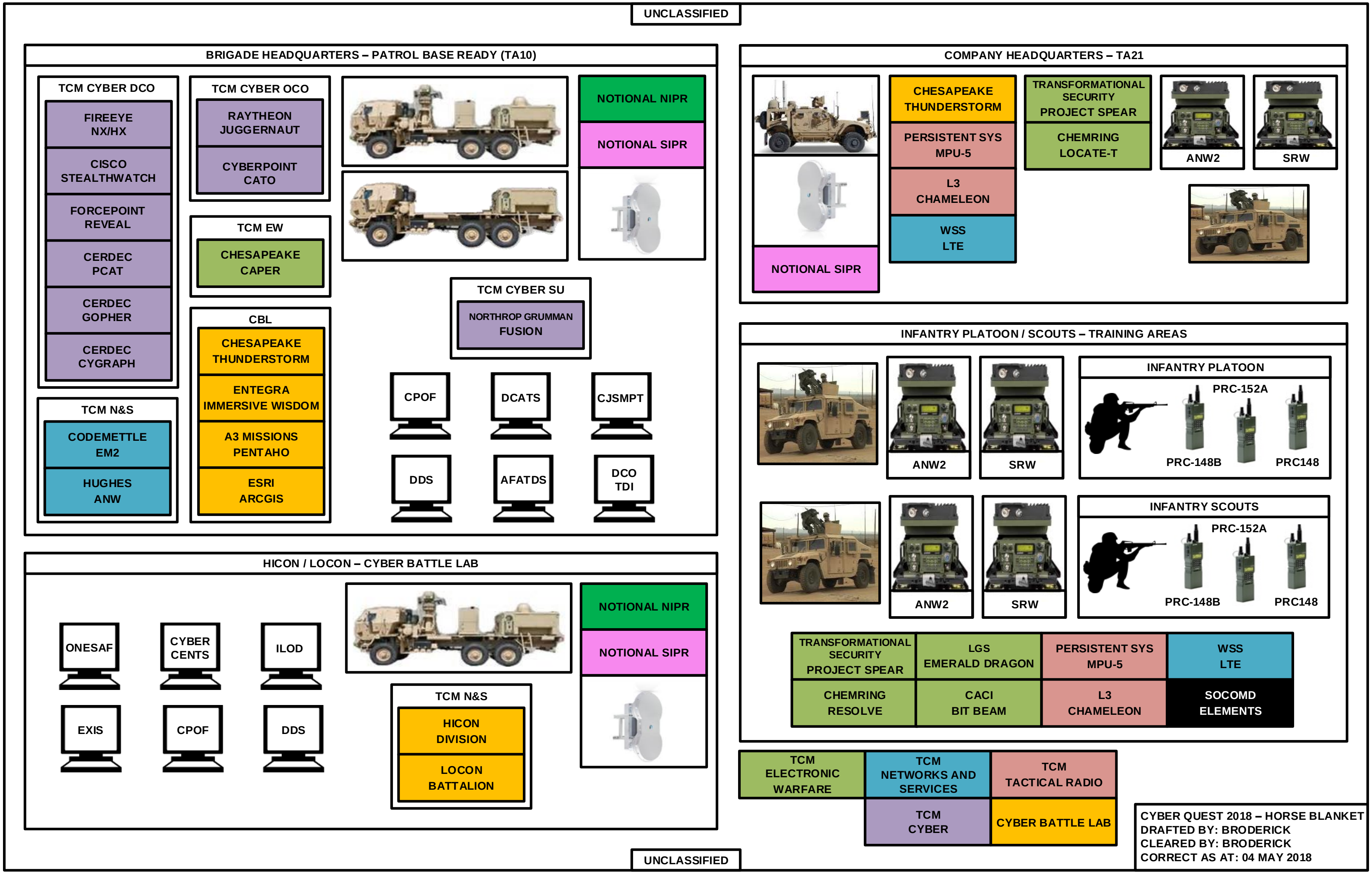
Pre-Decisional

Inform requirements, validate concepts & drive innovation via prototype assessments

CQ18 Sponsored Technology

Cyber Quest 2018 Participant (Capability)	Capability Description	Sponsor	Observer Controller Reqt
CACI (BITS BEAM)	EW Support (Sensor)	TCM EW	1 x EW SME Field & 1 x EW SME CO TOC
Chemring (Locate-T, Resolve)	EW Support (Sensor)	TCM EW	1 x EW SME Field & 1 x EW SME CO TOC
LGS (Emerald Dragon)	EW Support (WiFi/GSM DF)	TCM EW	1 x EW SME Field & 1 x EW SME CO TOC
Trans Security (Atom Defender)	EW Support (Sensor)	TCM EW	1 x EW SME Field & 1 x EW SME CO TOC
CTI (CAPER)	EW SU	TCM EW	1 x EWO SME BCT TOC
CERDEC (Cygraph)	**DCO** - Mission Mapping	TCM Cyber	1 x CYBER SME HICON
CERDEC (PCAT)	**DCO** - Analytics, Windows Monitor	TCM Cyber	1 x CYBER SME HICON
CERDEC (Gopher)	**DCO** - Host Analysis (Post Compromise)	TCM Cyber	1 x CYBER SME HICON
CISCO (Stealthwatch)	**DCO** Intrusion Detection	TCM Cyber	1 x CYBER SME HICON
Northrop Grumman (Fusion)	Cyber SU	TCM Cyber	1 X CYBER / CEMA SME BCT TOC
Fire Eye (NX/HX)	**DCO** Intrusion Detection	TCM Cyber	1 x CYBER SME HICON
Forcepoint (Reveal)	**DCO** (Insider threat/DLP)	TCM Cyber	1 x CYBER SME HICON
CyberPoint (CATO)	**OCO** (RF enabled Cyber)	TCM Cyber	1 x CYBER OCO SME BCT TOC & CO SITE
Raytheon (Juggernaut)	**OCO** (RF enabled Cyber)	TCM Cyber	1 x CYBER OCO SME BCT TOC & CO SITE
CodeMettle (EM2)	NETOPS	TCM N&S	1 X S6 NETWORK MANAGEMENT SME
WSS (LTE)	Tactical LTE Manpack	TCM N&S	2 X S6 TAC COMMS SME, CO Site / Ops
Hughes (LPI/LPD)	LPI/LPD (SATCOM)	TCM N&S	N/A
Persistent Systems (MPU5)	MANET Radio Capability	TCM TR	2 X S6 TAC COMMS SME CO Site / Ops
L3 (Chameleon)	LPI/LPD Tactical Radio	TCM TR	1 X S6 TAC COMMS SME, CO Site / Ops
Entegra (IM/VR)	Virtual Reality	CBL	Not Required
CTI (Thunderstorm)	EW Sensor Data Ingestion Engine	CBL	
A3 Missions (Pentaho)	Data Analytics	CBL	
US Army Special Operations Command	Offensive Cyber	CBL	Provided by USASOF
Strategic Command	Stand-off Offensive Cyber	CBL	Provided by STRATCOM

CQ18 Technology Laydown



UNCLASSIFIED

BRIGADE HEADQUARTERS – PATROL BASE READY (TA10)

TCM CYBER DCO
- FIREEYE NX/HX
- CISCO STEALTHWATCH
- FORCEPOINT REVEAL
- CERDEC PCAT
- CERDEC GOPHER
- CERDEC CYGRAPH

TCM N&S
- CODEMETTLE EM2
- HUGHES ANW

TCM CYBER OCO
- RAYTHEON JUGGERNAUT
- CYBERPOINT CATO

TCM EW
- CHESAPEAKE CAPER

CBL
- CHESAPEAKE THUNDERSTORM
- ENTEGRA IMMERSIVE WISDOM
- A3 MISSIONS PENTAHO
- ESRI ARCGIS

NOTIONAL NIPR

NOTIONAL SIPR

TCM CYBER SU
- NORTHROP GRUMMAN FUSION

CPOF, DCATS, CJSMPT, DDS, AFATDS, DCO TDI

HICON / LOCON – CYBER BATTLE LAB

ONESAF, CYBER CENTS, ILOD, EXIS, CPOF, DDS

NOTIONAL NIPR

NOTIONAL SIPR

TCM N&S
- HICON DIVISION
- LOCON BATTALION

COMPANY HEADQUARTERS – TA21

NOTIONAL SIPR

- CHESAPEAKE THUNDERSTORM
- PERSISTENT SYS MPU-5
- L3 CHAMELEON
- WSS LTE
- TRANSFORMATIONAL SECURITY PROJECT SPEAR
- CHEMRING LOCATE-T

ANW2, SRW

INFANTRY PLATOON / SCOUTS – TRAINING AREAS

ANW2, SRW

INFANTRY PLATOON

PRC-152A, PRC-148B, PRC148

ANW2, SRW

INFANTRY SCOUTS

PRC-152A, PRC-148B, PRC148

TRANSFORMATIONAL SECURITY PROJECT SPEAR	LGS EMERALD DRAGON	PERSISTENT SYS MPU-5	WSS LTE
CHEMRING RESOLVE	CACI BIT BEAM	L3 CHAMELEON	SOCOMD ELEMENTS

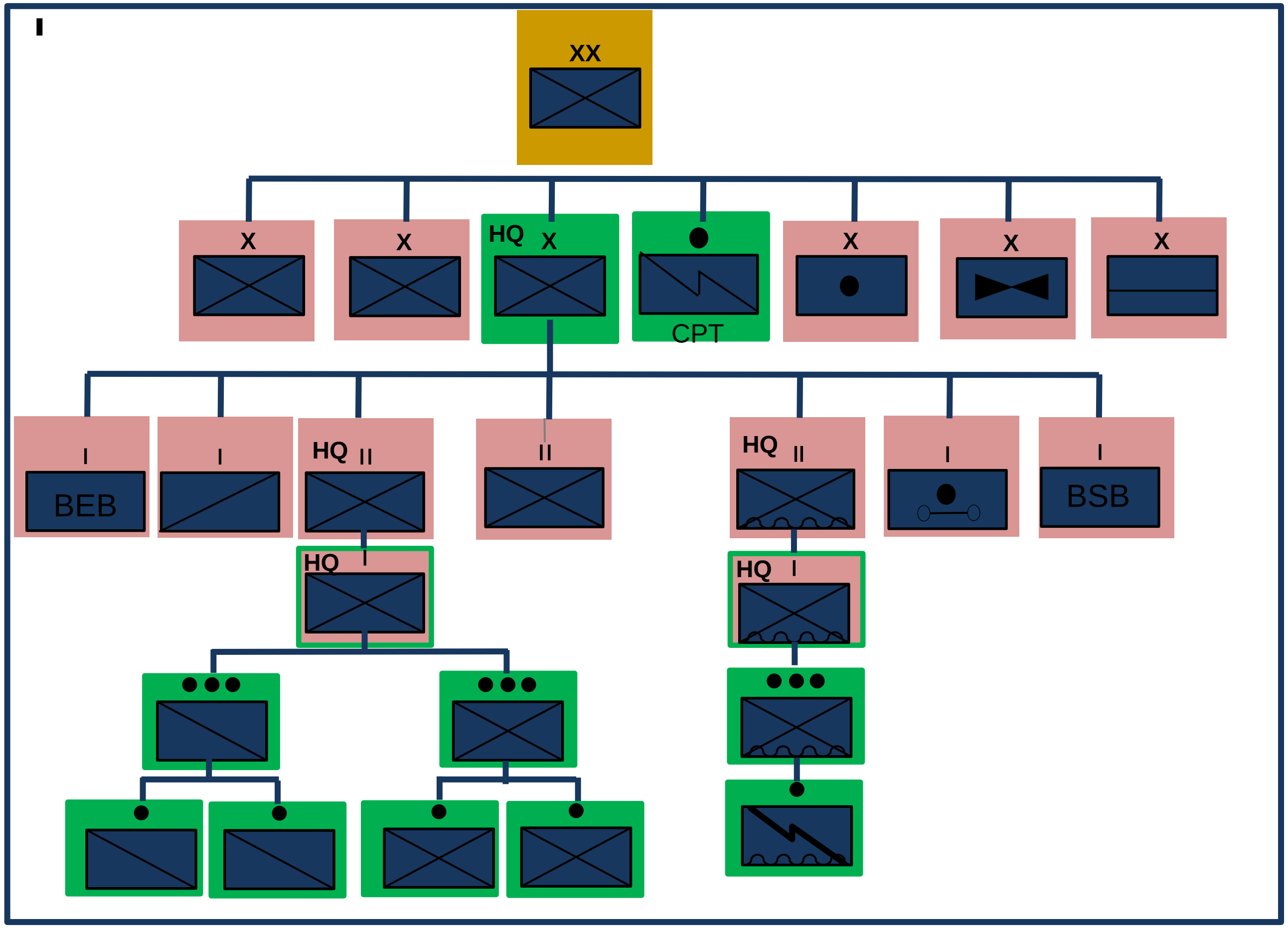
TCM ELECTRONIC WARFARE	TCM NETWORKS AND SERVICES	TCM TACTICAL RADIO
	TCM CYBER	CYBER BATTLE LAB

CYBER QUEST 2018 – HORSE BLANKET
DRAFTED BY: BRODERICK
CLEARED BY: BRODERICK
CORRECT AS AT: 04 MAY 2018

UNCLASSIFIED

Friendly Forces 'Exercise Play'

Task Organization

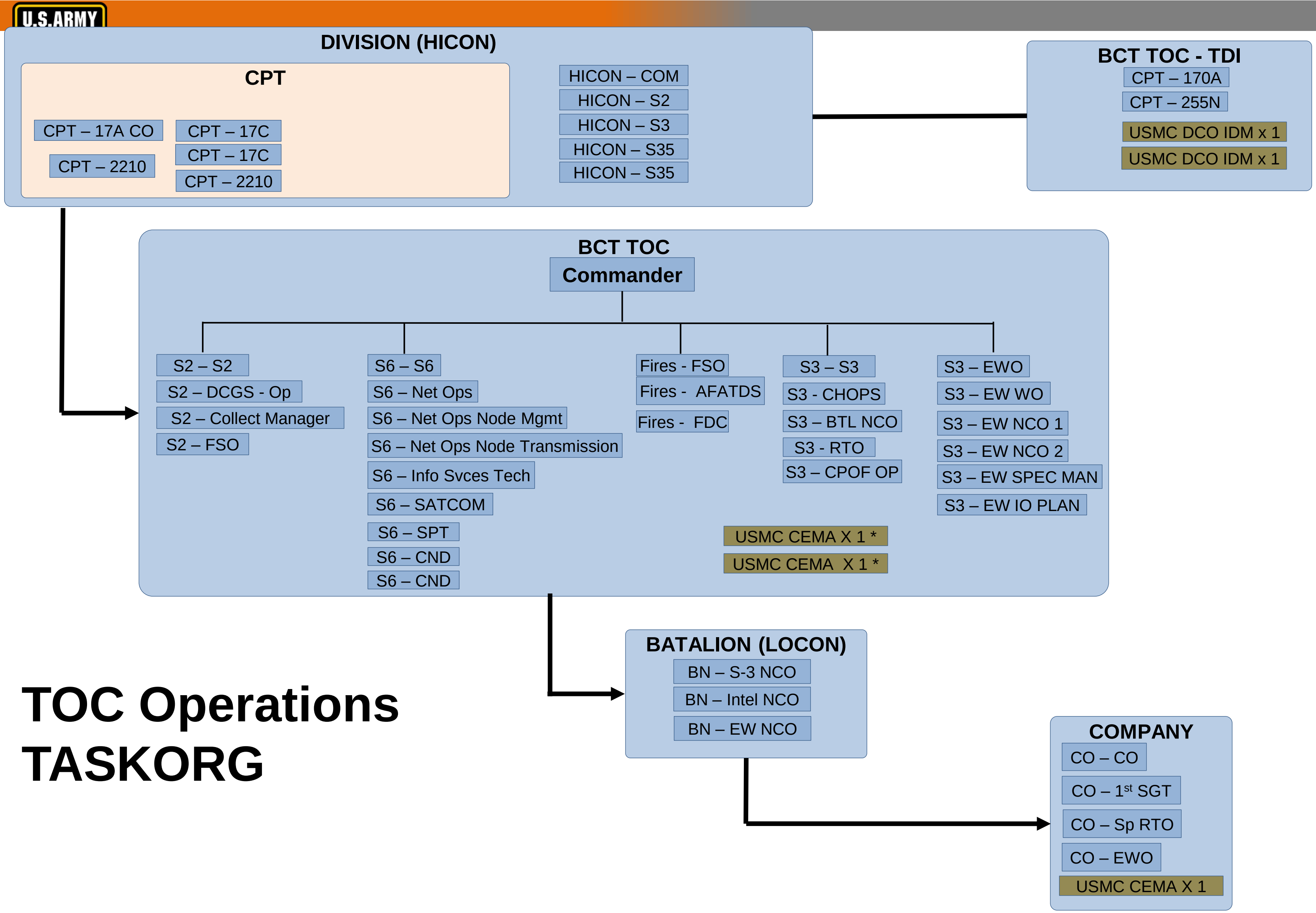


-- Live forces --

- BCT TOC with CEMA Cell and CPB Support.
- 1 x US Army Company TOC
- 1 x US Marine Company TOC (simulated)
- 1 x Scout Platoon
- 1 x Infantry Platoon
- 1 x USMC EW Team

- ***High Fidelity (green) – Live (Roleplayer/Modeled)***
- ***Medium Fidelity (amber) – Constructive (EXCON/HICON)***
- ***Low Fidelity (red) – Virtual (HICON/LOCON)***

Cyber Quest Actual Experiment Task Org



DIVISION (HICON)

CPT

CPT – 17A CO

CPT – 2210

CPT – 17C

CPT – 17C

CPT – 2210

HICON – COM

HICON – S2

HICON – S3

HICON – S35

HICON – S35

BCT TOC - TDI

CPT – 170A

CPT – 255N

USMC DCO IDM x 1

USMC DCO IDM x 1

BCT TOC

Commander

S2 – S2

S2 – DCGS - Op

S2 – Collect Manager

S2 – FSO

S6 – S6

S6 – Net Ops

S6 – Net Ops Node Mgmt

S6 – Net Ops Node Transmission

S6 – Info Svces Tech

S6 – SATCOM

S6 – SPT

S6 – CND

S6 – CND

Fires - FSO

Fires - AFATDS

Fires - FDC

S3 – S3

S3 - CHOPS

S3 – BTL NCO

S3 - RTO

S3 – CPOF OP

S3 – EWO

S3 – EW WO

S3 – EW NCO 1

S3 – EW NCO 2

S3 – EW SPEC MAN

S3 – EW IO PLAN

USMC CEMA X 1 *

USMC CEMA X 1 *

BATALION (LOCON)

BN – S-3 NCO

BN – Intel NCO

BN – EW NCO

COMPANY

CO – CO

CO – 1st SGT

CO – Sp RTO

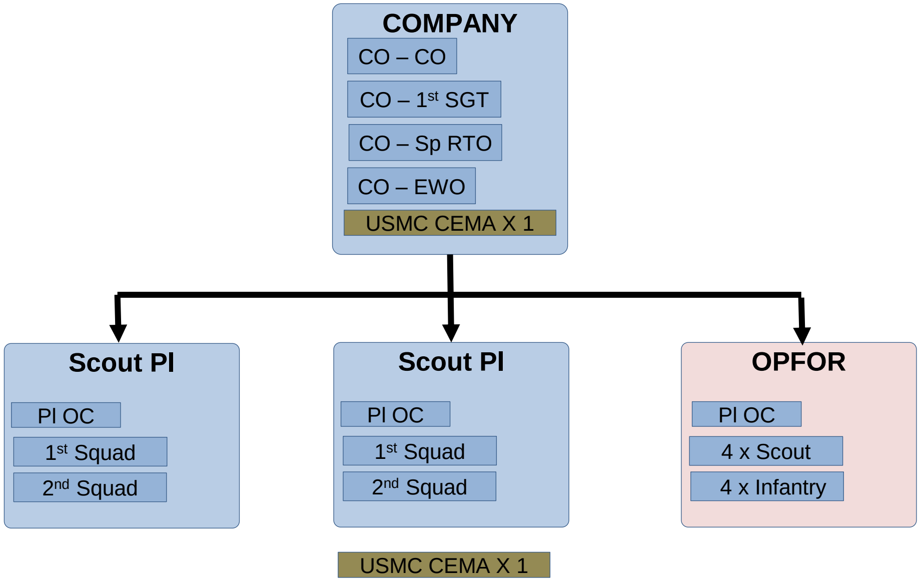
CO – EWO

USMC CEMA X 1

TOC Operations TASKORG

* **A**rmy **L**eaders' **C**yber **O**perations **C**ourse candidates

Cyber Quest Actual Experiment Task Org



COMPANY

CO – CO

CO – 1st SGT

CO – Sp RTO

CO – EWO

USMC CEMA X 1

Scout Pl

Pl OC

1st Squad

2nd Squad

Scout Pl

Pl OC

1st Squad

2nd Squad

USMC CEMA X 1

OPFOR

Pl OC

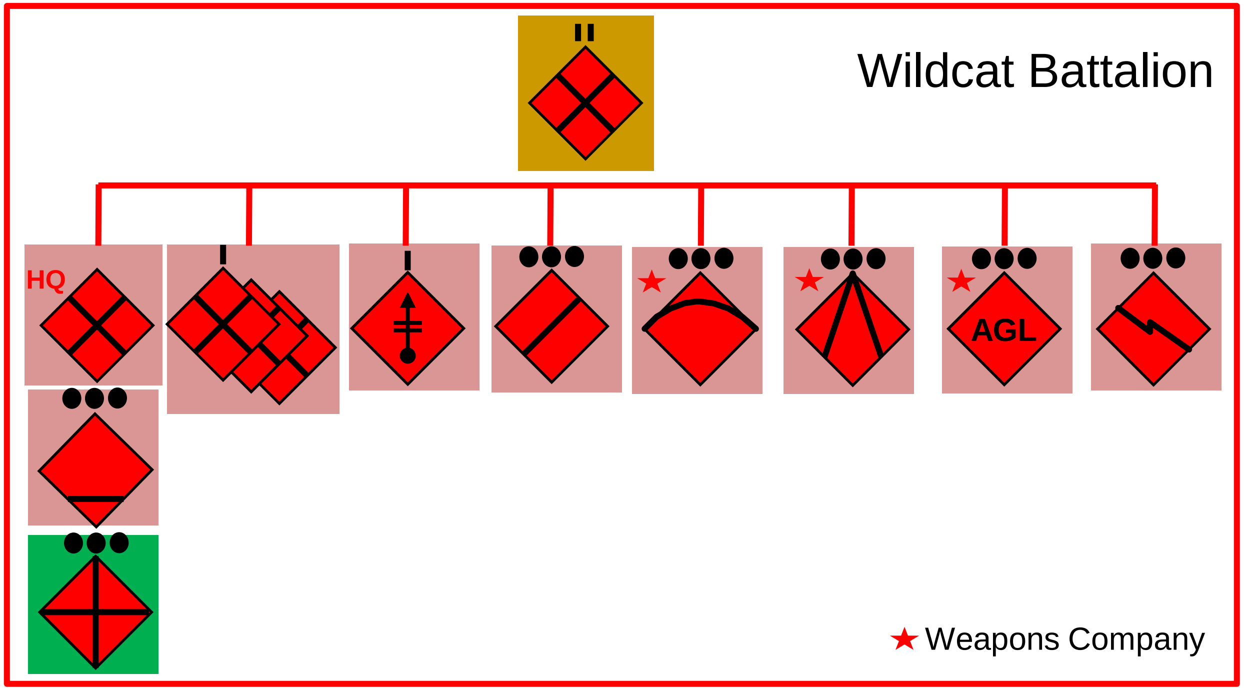
4 x Scout

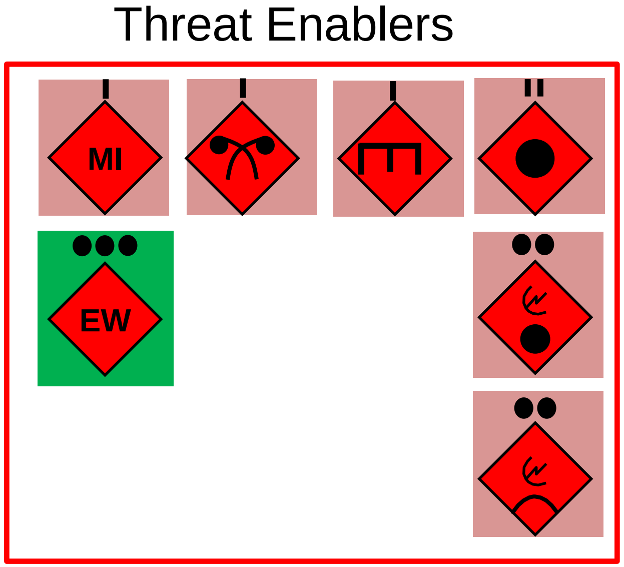
4 x Infantry

Field Operations TaskOrg

Exercise Threat Forces (Cyber Quest)

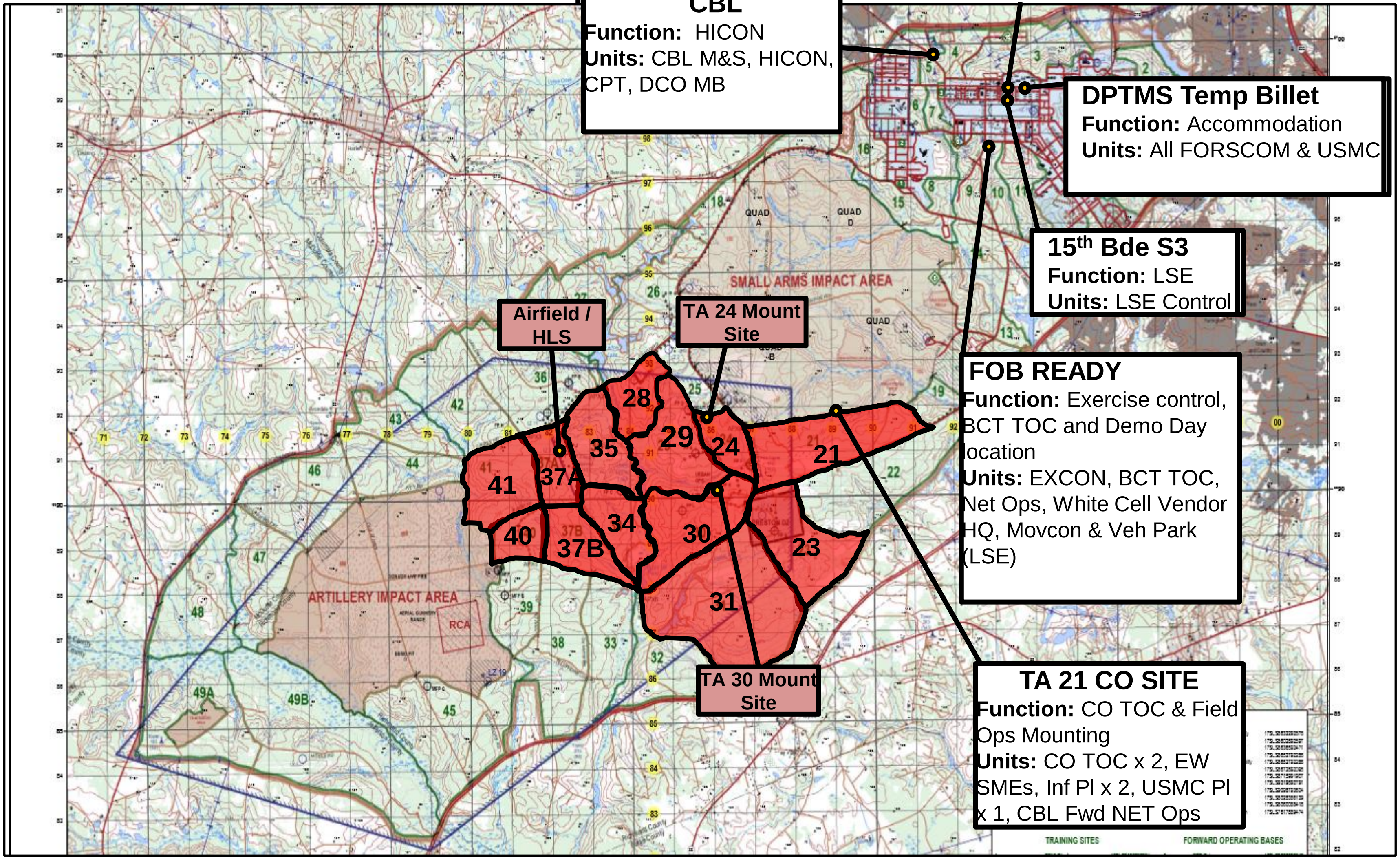
Task Organization





- ***High Fidelity (green) – Live (Roleplayer/Modeled)***
- ***Medium Fidelity (amber) – Constructive (EXCON/HICON)***
- ***Low Fidelity (red) – Virtual (HICON/LOCON)***

CQ18 Execution Locations – Fort Gordon



DFAC #6
Function: Breakfast & Dinner
Units: All FORSCOM & USMC

CBL
Function: HICON
Units: CBL M&S, HICON, CPT, DCO MB

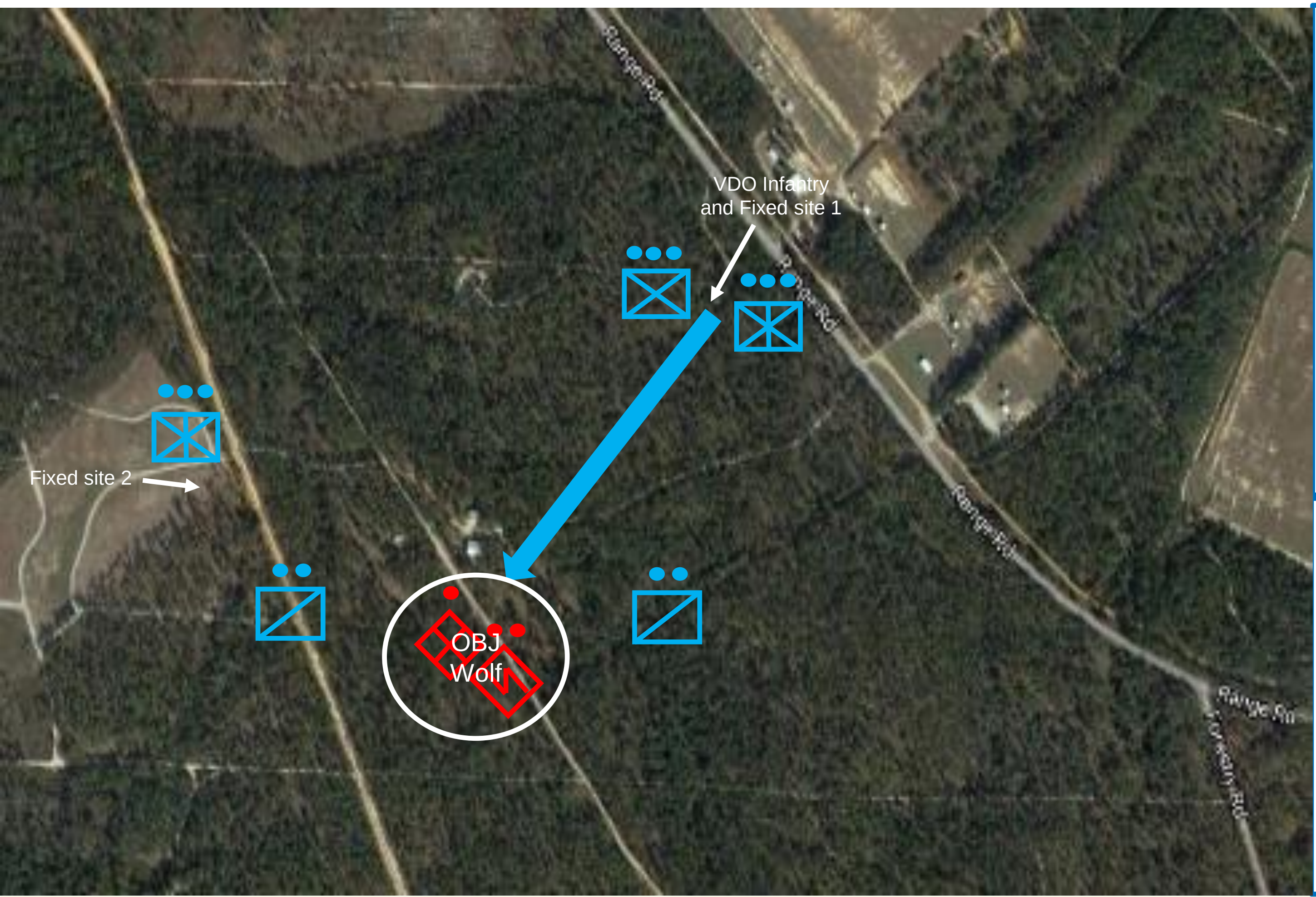
DPTMS Temp Billet
Function: Accommodation
Units: All FORSCOM & USMC

15th Bde S3
Function: LSE
Units: LSE Control

FOB READY
Function: Exercise control, BCT TOC and Demo Day location
Units: EXCON, BCT TOC, Net Ops, White Cell Vendor HQ, Movcon & Veh Park (LSE)

TA 21 CO SITE
Function: CO TOC & Field Ops Mounting
Units: CO TOC x 2, EW SMEs, Inf Pl x 2, USMC Pl x 1, CBL Fwd NET Ops

CQ18 Execution Example 1: Field Ops - EW Sensor Lane



SA Focus Areas Addressed

- ✓ Cyber SIGACTS
- Cyber Overlay
- ✓ Network Status (Friendly)
- ✓ Network Status (Threat)
- ✓ Emitters & Order of Battle
- Mission Impact
- ✓ Social Media

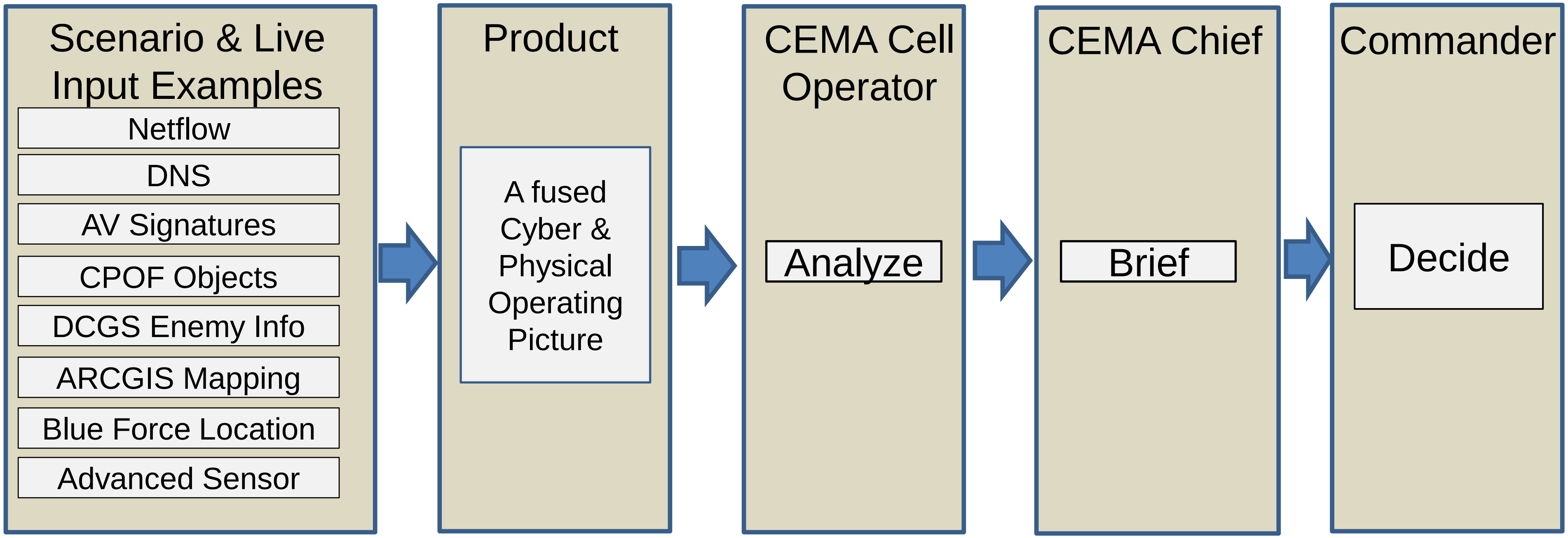
Vendors

- Chemring (Locate-T)
- Chemring (Resolve)
- Trans. Sec. (Atom Defender)
- CTI (Caper)

Mission: Conduct a deliberate attack on OBJ Wolf IOT destroy an enemy Comms element

CQ18 Execution Example 2: BCT TOC Example

Capability Gap: Cyber Situational Understanding



Scenario & Live Input Examples

- Netflow
- DNS
- AV Signatures
- CPOF Objects
- DCGS Enemy Info
- ARCGIS Mapping
- Blue Force Location
- Advanced Sensor

Product

A fused Cyber & Physical Operating Picture

CEMA Cell Operator

Analyze

CEMA Chief

Brief

Commander

Decide

SA Focus Areas Addressed

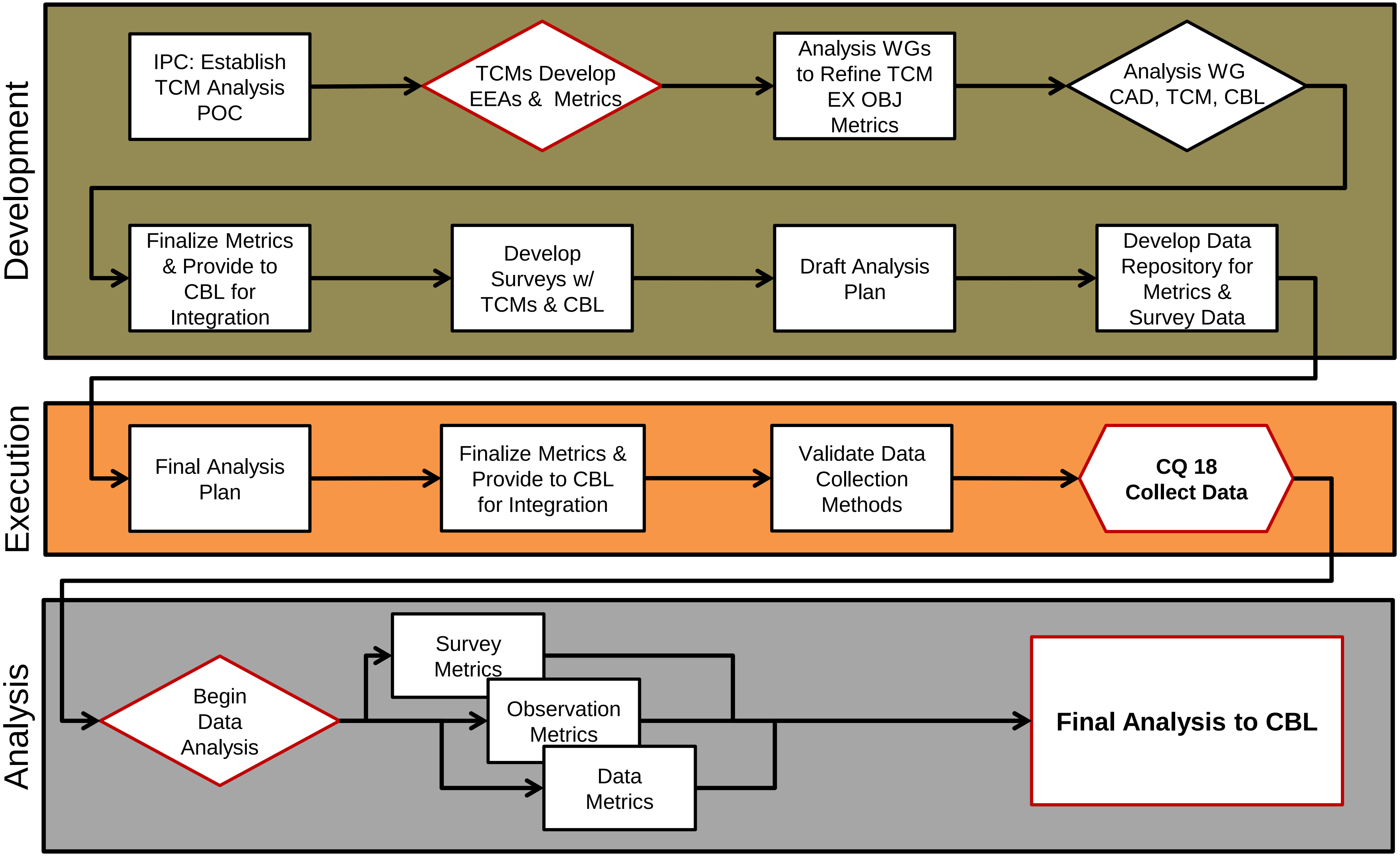
✓ Cyber SU

Vendors

- Northrop Grumman
- CERDEC

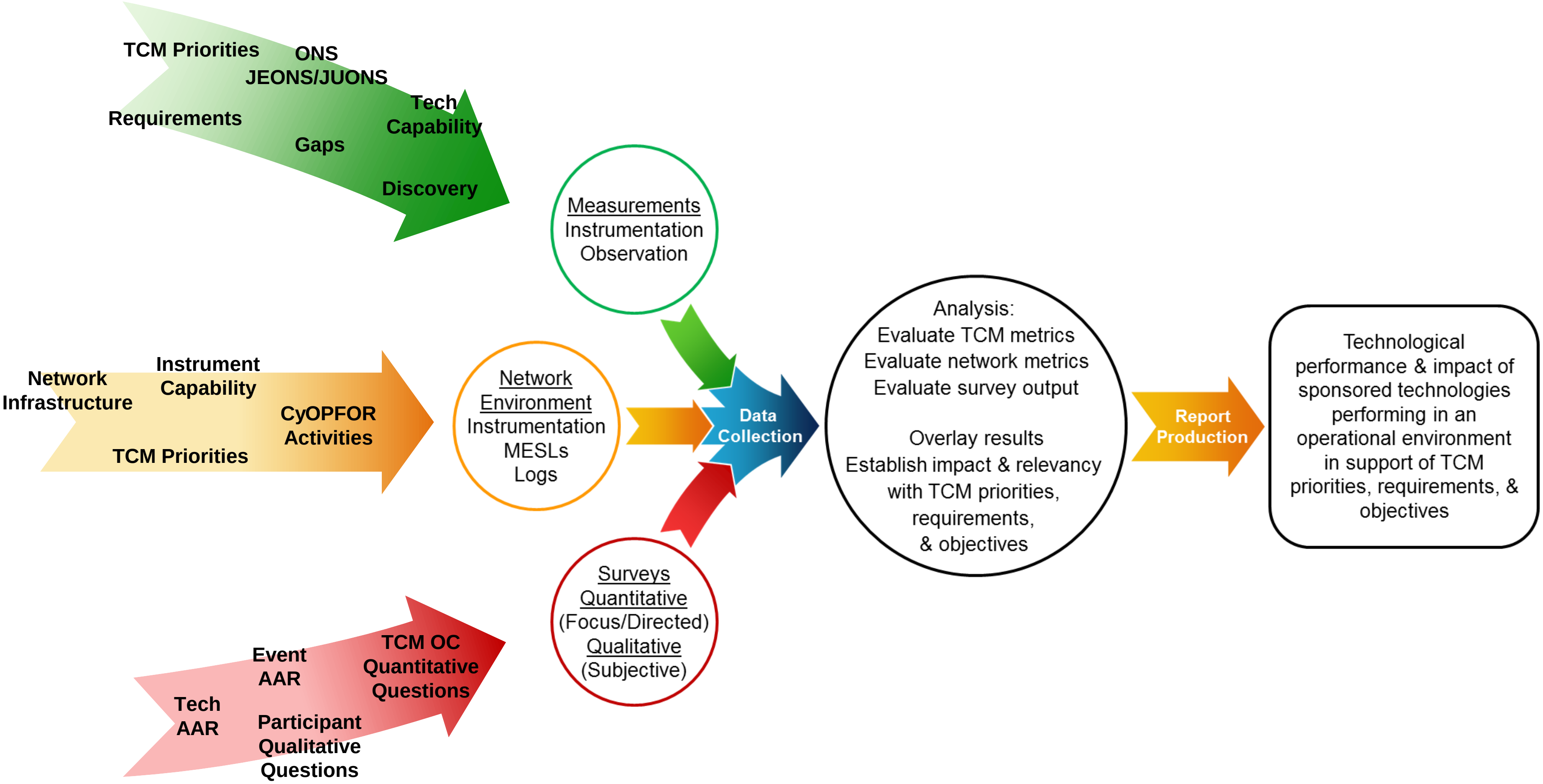
Objective: Provide the BCT Commander with the understanding required to support x-domain maneuver

CQ 18 Analysis Process - CAD


Development
IPC: Establish TCM Analysis POC
TCMs Develop EEAs & Metrics
Analysis WGs to Refine TCM EX OBJ Metrics
Analysis WG CAD, TCM, CBL
Finalize Metrics & Provide to CBL for Integration
Develop Surveys w/ TCMs & CBL
Draft Analysis Plan
Develop Data Repository for Metrics & Survey Data
Execution
Final Analysis Plan
Finalize Metrics & Provide to CBL for Integration
Validate Data Collection Methods
CQ 18 Collect Data
Analysis
Begin Data Analysis
Survey Metrics
Observation Metrics
Data Metrics
Final Analysis to CBL

CQ 18 Analysis Process - CAD

EEA → Metrics | Data | Analysis | Output



TCM Priorities
ONS
JEONS/JUONS
Requirements
Tech Capability
Gaps
Discovery

Network Infrastructure
Instrument Capability
CyOPFOR Activities
TCM Priorities

Event AAR
Tech AAR
TCM OC Quantitative Questions
Participant Qualitative Questions

Measurements
Instrumentation
Observation

Network Environment
Instrumentation
MESLs
Logs

Surveys
Quantitative
(Focus/Directed)
Qualitative
(Subjective)

Data Collection

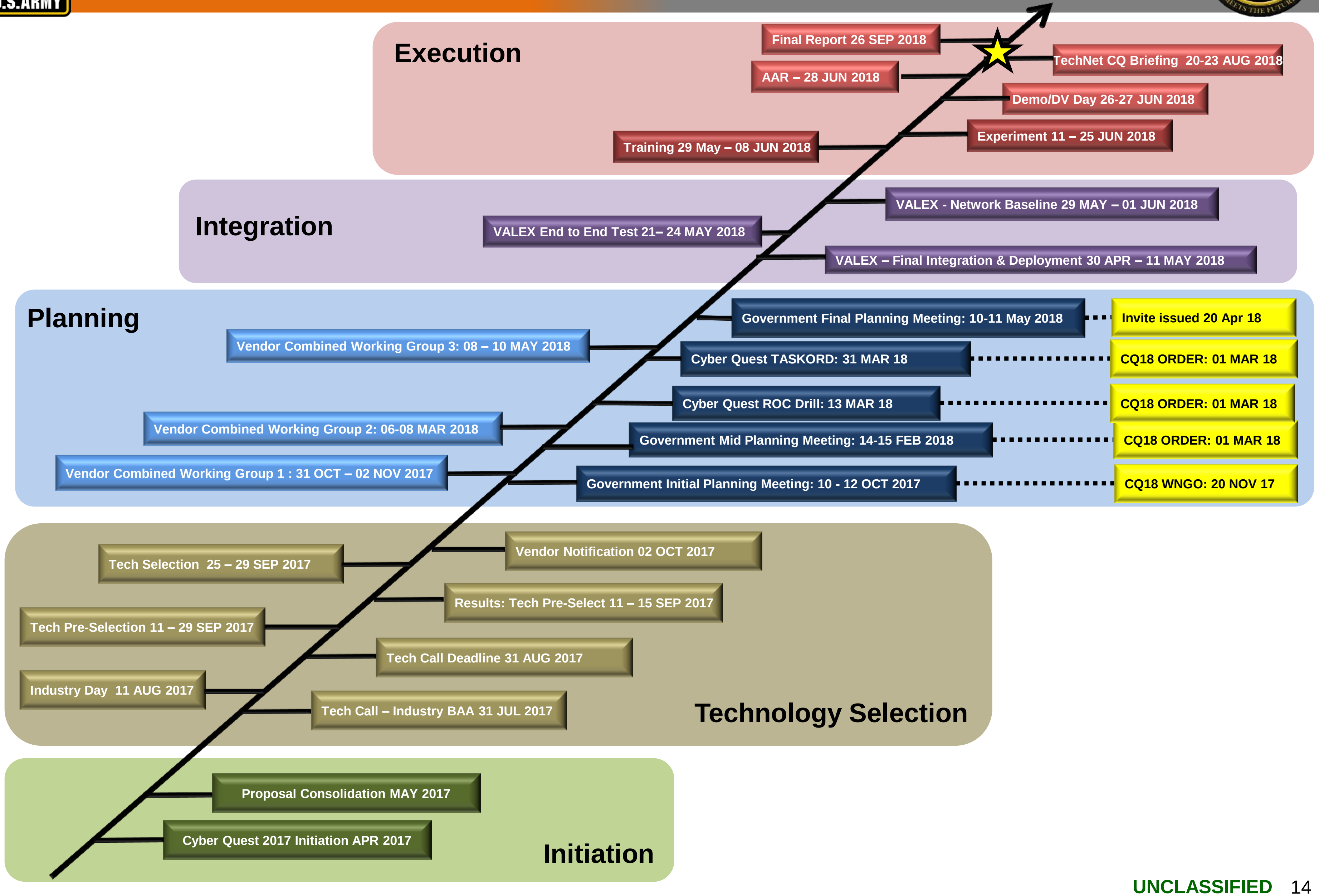
Analysis:
Evaluate TCM metrics
Evaluate network metrics
Evaluate survey output

Overlay results
Establish impact & relevancy with TCM priorities, requirements, & objectives

Report Production

Technological performance & impact of sponsored technologies performing in an operational environment in support of TCM priorities, requirements, & objectives

CQ18 Timeline



Execution

Final Report 26 SEP 2018

TechNet CQ Briefing 20-23 AUG 2018

AAR – 28 JUN 2018

Demo/DV Day 26-27 JUN 2018

Experiment 11 – 25 JUN 2018

Training 29 May – 08 JUN 2018

Integration

VALEX - Network Baseline 29 MAY – 01 JUN 2018

VALEX End to End Test 21– 24 MAY 2018

VALEX – Final Integration & Deployment 30 APR – 11 MAY 2018

Planning

Government Final Planning Meeting: 10-11 May 2018 — Invite issued 20 Apr 18

Vendor Combined Working Group 3: 08 – 10 MAY 2018

Cyber Quest TASKORD: 31 MAR 18 — CQ18 ORDER: 01 MAR 18

Cyber Quest ROC Drill: 13 MAR 18 — CQ18 ORDER: 01 MAR 18

Vendor Combined Working Group 2: 06-08 MAR 2018

Government Mid Planning Meeting: 14-15 FEB 2018 — CQ18 ORDER: 01 MAR 18

Vendor Combined Working Group 1 : 31 OCT – 02 NOV 2017

Government Initial Planning Meeting: 10 - 12 OCT 2017 — CQ18 WNGO: 20 NOV 17

Technology Selection

Vendor Notification 02 OCT 2017

Tech Selection 25 – 29 SEP 2017

Results: Tech Pre-Select 11 – 15 SEP 2017

Tech Pre-Selection 11 – 29 SEP 2017

Tech Call Deadline 31 AUG 2017

Industry Day 11 AUG 2017

Tech Call – Industry BAA 31 JUL 2017

Initiation

Proposal Consolidation MAY 2017

Cyber Quest 2017 Initiation APR 2017