CYBER YANKEE 2019

(CY19)

August 3-10, 2019

AFTER ACTION REPORT/IMPROVEMENT PLAN

VERSION 1.0

Published:

04 February 2020

This page is intentionally blank.

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is Cyber Yankee 2019 (CY19) 3-10 August 2019 - AAR/IP.

2. The information gathered in this AAR/IP will drive future planning of regional cyber exercises. Sharing this document across government agencies seeking information on cyber exercise planning is encouraged.

3. Points of Contact:

   Cyber Yankee Exercise Director: LTC Woody Groton, G6 NHARNG, barry.w.groton.mil@mail.mil (603) 225-1201

   Cyber Yankee Deputy Exercise Director: LTC Richard Leydon, G6 CTARNG, richard.leydon.mil@mail.mil (860) 524-4916

   Cyber Yankee White Cell OIC: COL Mike Tetreault, G6 RIARNG, roland.m.tetreault.mil@mail.mil (401) 714-9733

   Cyber Yankee Assessment Lead: COL David Yasenchock, FEMA Region One - Army CREPLO, david.a.yasenchock.mil@mail.mil (210) 557-0222

   Senior Army National Guard Advisor to United States Cyber Command, COL Richard Berthao, richard.berthao.mil@mail.mil, (443) 634-5443

This page is intentionally blank.

CONTENTS

This page is intentionally blank.

EXECUTIVE SUMMARY

The goal of Cyber Yankee 2019 was to continue the successful execution of a realistic cyber exercise for Army National Guard Defensive Cyberspace Operations Elements (DCOE) and other Cyber units to further train and apply their skills as cyber defenders. This year, we also integrated the several agencies from the State of New Hampshire, the 229th COS, additional legal support, and elements of the 91st Cyber Brigade. Exercise planners used lessons learned from Cyber Yankee 2015-2018 to improve the exercise. The exercise focused on developing strong collaboration across all of the New England Cyber elements, state, and federal government partners in cyber defense. Cyber Yankee '19 was part of the Federal Emergency Management Agency (FEMA) National Exercise Program.

Cyber Yankee 19 emphasized learning key skills in cyber defense and reporting within an Inter-service and Inter-agency operational environment providing a more realistic scenario that incorporated threat intelligence, associated cyber threats, and associated Tactics, Techniques and Procedures (TTPs). The exercise also linked TTPs with exercise adversary actions (Technical, Operational, and Ideological).

The role of information sharing in Cyber Yankee continued to be a major factor in the exercise. Intelligence Soldiers and Airmen analyzed information reported on notional threats according to most likely and most dangerous courses of actions against friendly cyber first responders and their supported mission partners. The scenario used known realistic threat actions existing in today's operational environment to support exercising prescribed battle drills. A live opposing force executed actions simulating each notional enemy threat and action. These included; traditional nation state intelligence assists (HUMINT), cybercriminals, terrorist organizations, information operations threats, and kinetic actors. Each notional threat actor is associated with a set of Tactics, Techniques, and Procedures (TTPs) that correlate to specific technical, operational, motivational, operational, and capability-based signatures in order to allow friendly forces the analyze, assess, attribute, and mitigate threat technical and operational actions in assigned areas of operation. Cyber defenders provided threat indicators of compromise (IOC) to the National Guard Bureau and U.S. Cyber Command Joint Operations Center via automated tools. The Electricity, Water, and Multi-State Information Sharing and Analysis Centers participated to provide an additional channel for information sharing and incident response support.

A robust collection of mission partners from state government as well as critical infrastructure and key resources (CI/KR) in the region enhanced the realism of the exercise. National Guard cyber responders had to work with their supported mission partners in a manner similar to what they would experience in a real world scenario. Judge Advocate General support was robust providing legal guidance and rules for the use of cyber. This support would be critical in an actual incident and is an area identified as one of the leading requirements by the National Guard Cyber Capabilities Assessment Study. Additionally, for the first time general counsel from the supported state government and CI/KR participated providing input on memoranda of understanding and non-disclosure agreements. New Hampshire state government had a robust

participation to include the Department of Information Technology, Department of Transportation, fusion center, and state emergency operations center. The New Hampshire National Guard Joint Operations Center participated in Cyber Yankee as part of the Granite Guard National Guard Civil Support exercise.

The end state was continued development of a more robust capacity and capability for the Defensive Cyberspace Operations Elements and other Guard and Reserve cyber units in the New England states as well as a growth in partnerships across multiple levels of government throughout the region. Conducting the exercise at the unclassified level (leveraging open source intelligence information) ensured maximum relevant and current training for all government and non-government participants.

Regional Focus

Cyber Yankee compared to other national level exercises:

- Need for a regional focus versus a national focus with limited local aspects
- Size and Cost (strong value)
- Venue/Location (central in New England)
- National Guard forces are Title 32/State Active Duty focused
- Scenario is based on State Government and critical infrastructure and key resources (CI/KR) Support Missions
- Leverage and strengthen New England cyber working groups relationships

Major Strengths/Sustain

The major strengths identified during this exercise are as follows:

- Cyber Yankee is a regionally focused exercise building upon relationships between the various National Guard, federal government, state government, and industry partners in New England. A regional exercise is cost effective and better facilitates cooperation among the various participants. Travel for planning conferences and exercise execution is within 3 hours for most participants.
- Cyber Yankee remains focused on collective training. We continued to emphasize individual/classroom training should be prior to the exercise and not during, although we do offer additional training and classes during pre-time and after range hours.
- Use of the 91st Cyber Brigade ShadowNet range to provide a simulated network for each exercise enclave. ShadowNet represents the best range simulation environment for cyber exercises as it is built and maintained by experienced cyber Soldiers and Airmen.
- The use of ICS/SCADA simulations enhance the training environment.
- Information sharing with industry partners.
- Inclusion of industry partners during the exercise planning process.
- Maintain the exercise in the UNCLASS real to better support partnerships.
- Continue to integrate new techs into the Range (Hive-IQ, Unity, MatterMost, DAART, and Slack).
- The size of the exercise is manageable and provides for cooperation, learning, and team building.
- Continue to provide industry partners and other to be part of the Red team.
- The use of Emergency Management and Assistance Compact (EMAC) and the participation of a State from outside our Region provided a training opportunity to exercise Joint Reception, Staging, and Onward Integration (JRSOI) of cyber forces. The DCOE team from Alabama with their industry partner participated replicating EMAC support from outside the effected region.
- Training on software tools prior to the exercise facilitated execution.
- Working with Industry Partners was very beneficial. Industry partners seemed prepared and were able to provide us with adequate information. Each enclave had an average of

10 industry partners providing a realistic problem set for Blue team responders.
- Treating the exercise as more of a training and learning event and less of a competition made it much easier for the teams to learn.
- Cross leveling of technical resources from the Red cell and blue team to facilitate accelerated mission execution.
- Participation from active duty elements of the Cyber National Mission Force facilitated the training and provided an opportunity to share best practices. Cyber Yankee provides the CNMF with an opportunity to train on cyber incident response outside the Department of Defense Information Network (DODIN).
- Participation from Information Sharing and Analysis Centers (ISAC) provides an opportunity for military and industry partners to exercise information sharing from these entities. The Electricity ISAC provided a senior analyst for the duration of the exercise greatly enhancing information sharing.
- Support from the Persistent Cyber Training Environment Program Office (PCTE) as a first use event.

Primary Areas for Improvement

There were several opportunities for improvement in the exercise.

- Use of/reliance on Slack as an operational mission command system was not a realistic tool for a real-world event.
- Use of the Persistent Cyber Training Environment as a way ahead for funding.
- OPSEC/Counterintelligence gaps exist due to limited resources.
- The use of the terminology regarding “intelligence” vs “information sharing”. Intelligence shuts doors, implicates legal authorities and creates potential PR issues. We are sharing “information” and “awareness”. Need to follow that Information Awareness & Assessment doctrinal terminology used by NG-J2 imagery support to DOMOPs (known as UPAD = Unclassified Processing, Assessment & Dissemination).
- Lines of Communication with external partners (e.g., State JOC, State Police, etc.) need to be tested and practiced prior to event.
- Teams should arrive at the exercise with Standard Operating Procedures and draft memoranda of agreements to facilitate timely support to the incident.
- Coordination of simulation of the industry partner’s IT environment prior to the exercise will facilitate realism and allow industry partners to work in a familiar environment.
- Provide a better picture and brief of the network to the industry partners including items like, employee list, network diagrams, topology and tools on the network.
- Exercise control should provide improved linkage between Red and White cells to synchronize the rubric and effects.
- Establish contracts earlier to better develop the range.
- Improve daily mission planning for all participants.
- Increase the time for hot washes between the Blue and Red teams daily to demonstrate the attacks and talk about possible fixes. Provide time either before the beginning of the

exercise or on the final day to demonstrate attacks and what the indicators of such attacks were.

- Allocate more time to range validation in order to ensure everything is working prior to the start of the exercise.
- Test how communication and tracking processes that would be used in a real incident.
- Include PAO's to help with "misinformation" – Information Ops IO.
- Having a training week prior to execution allows for individual training, team preparation, and communications rehearsals.

Overall, this exercise successfully met the established goals and objectives of the regional cyber teams. Future exercises within the region should continue as well as formalizing a regional model for the entire nation.

SECTION 1: EXERCISE OVERVIEW

Exercise Details

Exercise Name
Cyber Yankee 2019

Type of Exercise
Tactical Cyber Training Range Exercise

Exercise Start Date
August 5, 2019

Exercise End Date
August 9, 2019

Duration
Ten (10) Hour Days (Including meal rotation)

Location
Regional Training Institute, New Hampshire Army National Guard, Edward Cross Training Complex.

Supporting Elements
91st Cyber Brigade hosted the ShadowNet range.

Goals and Objectives

The goal of Cyber Yankee 2019 is to create a realistic cyber exercise for Army National Guard Cyber Teams and related Air National Guard personnel 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.

Emphasis is on learning key skills in cyber defense and reporting within an Inter-service and Inter-agency operational environment.

End State

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 and industry.

Capabilities
Cyber Defense, Information Sharing and Partnership Development

Scenario Type
Cyber Attacks

Participating Organizations

Military and Government Agency participants:

- Defensive Cyberspace Operations Element (DCOE):
  - Massachusetts Army National Guard
  - New Hampshire Army National Guard
  - Rhode Island Army National Guard
  - Vermont Army National Guard
  - Alabama Army National Guard
  - Connecticut Army National Guard
- 91st Cyber Brigade
- 126th Cyber Protection Battalion
- 146th Cyber Detachment Connecticut Army National Guard
- 101st Communications Flight, Maine Air National Guard
- 103rd Air Wing, Connecticut Air National Guard
- 103rd Air Control Squadron, Connecticut Air Nation Guard
- 157th Communications Flight, New Hampshire Air National Guard
- 224th ADG, New York Air National Guard
- 229th Cyberspace Operations Squadron, Vermont Air National Guard
- 102nd Network Warfare Squadron, Rhode Island Air National Guard
- 173 CPT, New York Army National Guard
- Defense Coordinating Element, Region One (New England) Army and Air Force Reserve
- Massachusetts Information Operations Field Support Team
- 102nd Intelligence Surveillance Reconnaissance Group, Massachusetts Air National Guard
- 195th Regiment NH Regional Training Institute (RTI)
- 2-124th VT RTI (Information Operations)
- Delaware Air National Guard
- 19th Airlift Wing
- United States Cyber Command
- Cyber National Mission Force Task Force 5 (02 CPT, 62 NCPT, 82 CPT, & 90 CPT)
- 41 IS/DOT
- Portsmouth Naval Shipyard
- Department of Homeland Security
- Federal Energy Regulatory Commission
- New Hampshire Department of Information Technology
- New Hampshire Department of Transportation
- New Hampshire Homeland Security/Emergency Management
- New Hampshire State Police
- Massachusetts Emergency Management Agency
- Massachusetts Executive Office of Public Safety
- Maine Emergency Management Agency

Critical Infrastructure:

- Metropolitan Water District (MDC) Hartford, CT
- Massachusetts Water Resource Authority
- Avangrid
- Eversource
- ISO New England
- Southern Company
- Southern New Hampshire Medical Center
- Elliot Health System
- Vermont Electric Cooperative

Industry and Academic Support:

- Kennebunk Cyber
- Massachusetts Institute of Technology/Lincoln Laboratory
- Metova
- MITRE
- Nusura
- Teamworx Security
- Tenable
- Wapack Labs

Number of Participants (CY 2018 stats in brackets)

- Total Participants: 300 ⇑ (184)
- Players: 121 ⇑ (81)
- Observers/Assessors/Controllers: 14 (18)
- JAG: 7 ⇑ (4)
- JOC / Fusion Center: 20⇑ (10)
- Industry Reps / Other Agency: 64 (12)
- Exercise Support: 39 ⇑ (38)
- Distinguished Visitors: over 100 ⇑ (87)

SECTION 2: EXERCISE DESIGN SUMMARY

Exercise Purpose and Design

- Focus on training cyber defense team battle drills via us of Blue Team Standard Operating Procedures (SOPs) & Tactics, Techniques, and Procedures (TTPs)
- Focus on Blue Team Field Manual (BTFM) validation and TTP development
- Ensure integration of intelligence analysts
- Use traditional red (attack), blue (defend), white (evaluate) cell operational process
- Leverage a small unit training versus a larger model
- Validate cyber defense concepts and skills
- Validate cyber training models that work within drill weekend and Annual Training periods
- Validate the state guard's ability to respond to a cyber incident involving state, local agencies, and industry partners

Exercise Objectives, Capabilities, and Activities

Cyber Yankee had several objectives, capabilities, and activities. Each of these training models focused on the tactical level cyber defense teams. Training remained at the technical level. However, this year achieved high integrated of intelligence and operations into the training. Exercise leadership and evaluators routinely stressed an operational focus to all blue team participants as an essential compliment to the hands-on technical mission aspects.

Based upon the identified exercise objectives below, the exercise planning team decided to demonstrate the following capabilities during this exercise:

- **Objective 1: Planning** – Evaluate each cyber team's integration into the operational planning process.
- **Objective 2: Collaboration** – Effective and efficient collaboration between the CND-Ts at a Regional level in conjunction with industry and government agency interaction.
- **Objective 3: Learning** – ensure the exercise in conducted in a "learning" format and not just an evaluation or team competition.
- **Objective 4: Cyber Operations and Intel Exercised** – Integrate operations (Joint Operations Center) and intelligence personnel into exercise missions.
- **Objective 5**: **Validate BTFM, TTPs, SOPs** – Are the existing manuals and SOPs sufficient and are they being used by the teams effectively?

Scenario Summary

- Cyber Yankee 2019 takes place during a hurricane that hits the New Hampshire Seacoast in Portsmouth. The hurricane causes flooding, water and power outages. A civil disturbance results from frustration with power outages and lack of access to ATMs.

- The Krasnovian Government has been the object of United Nations sanctions and uses the hurricane event to mask cyber attacks against critical infrastructure and state government as part of a campaign to sow distrust in the government's ability to support its citizens.

- The New Hampshire State Emergency Operations Center is activated in response to the incident. National Guard cyber forces are activated to assist with response to cyberattack against state government and critical infrastructure. New Hampshire executes emergency management assistance compacts to bring in additional Guard support from Massachusetts, Rhode Island, Connecticut, and Alabama.

- A transnational criminal organization from Eastern Europe conducts cyberattacks to take advantage of the situation.

SECTION 3: ANALYSIS OF CAPABILITIES

This section reviews performance observations of the exercised capabilities, activities, and tasks. The capabilities listed come from the exercise objectives of Cyber Yankee 2019. The observations for each listed capability feed into the improvement plan located in Appendix A.

Capability 1: Planning

Capability Summary: Cyber teams planning capability has improved since Cyber Yankee 18. Newer team leaders need more experience planning their missions from an operational perspective. They accomplished their missions from a technical perspective but they often overlooked basic leadership tasks in terms of task organization, delegation, and reporting.

Capability 2: Intelligence/Information Sharing and Dissemination

Capability Summary: Initial INTSUMS were weak and not to standard but improved throughout the exercise. Intel analysts were proficient at providing cyber spot reports to the JOC/Fusion center. Hive IQ facilitated information sharing between blue teams and JOC/Fusion.

Capability 3: Defensive Cyberspace Operations Element (DCOE) Operations

Capability Summary: The DCOEs demonstrated adequate training and performance on basic cyber defense operations. This is an area where teams performed well at the individual and technical levels.

Capability 4: Operating Procedures and Playbook

Capability Summary: Primary Team references include the Cyber Protection Team Crew Manual, Blue Team Field Manual, the DCO-E Battle Drills, and local SOPs. The CJCSM 6510.01B, "Cyber Incident Handling" needs to be included as a key reference.

Capability 5: Communications and Reporting

Capability Summary: A key training aspect of the exercise was improvement of communications and reporting. Both the blue teams and the JOC/Fusion center collaborated on developing and improving communications and reporting tools and techniques. While both elements learned to expedite and improve their reporting and communications methods, it was evident that reporting of cyber incidents and missions needs to be improved. There are multiple reporting methods across all levels of government. Many of these reports (especially within DoD and law enforcement) are classified and of no use to teams supporting civilian organizations in an unclassified environment. Reporting tools and techniques must be refined for use by reserve component cyber teams.

Capability 6: Industry and Agency Participation and Support

Capability Summary: Cyber Yankee has the best industry partner to military player

ration of any exercise. This greatly improves realism. Extensive support from our federal government partners during the planning and execution of Cyber Yankee enhanced training outcomes. Support from JOC and state EOC staff would enhance the realism of the exercise but is difficult to obtain this support.

Capability 7: Cyber Range Operations and Support

Capability Summary: An important success of Cyber Yankee was the ShadowNet cyber range support provided by the 91st Cyber Brigade. The range design and functionality met all training requirements of the exercise. Both technical design prior to and technical support during the exercise were excellent. Exercise participants agreed that the range was among the best training ranges they have used. Inclusion of a security baseline in the enclave provided a more realistic range environment for blue players and supported industry partners.

Capability 8: Red Team Operations

Capability Summary: The exercise red team was a composite of Army and Air National Guard, Army Reserve and industry personnel. Their performance was admirable for an ad-hoc team stood up for this exercise. An important take-away from this exercise was the full integration of the red team with the exercise white cell and intel/scenario development team. By having flexibility to dynamically adapt to training requirements, the red team was an effective training tool for the blue teams. The concept of white cell assessments and embedded observers feeding training objective information to exercise control (also white cell) and then the red cell enabled maximization of training objectives. This approach ensured adjustments in real time to minimize team frustration and maximize training and learning objectives and opportunities.

Capability 9: Integration of Title 10 DOD Cyber National Mission Force (CNMF)

Capability Summary: Cyber Yankee 19 was the second year that included a Title 10 (Active Duty) training opportunity. Cyber operators from four CNMF Cyber Protection Teams supported defensive cyberspace operations support to the two critical infrastructure enclaves. If an incident exceeds local capacity Title 10 cyber operators may be tasked through DHS mission assignments. This would then require a National Guard Dual Status Commander. During the exercise, the active duty cyber operators integrated well with the National Guard Soldiers and Airmen. Additionally CNMF staff supported the Joint Operations Center and White Cell for enhanced coordination. Recommend CNMF continue to participate in order to better prepare for contingencies.

SECTION 4: CONCLUSION

The design and execution of Cyber Yankee 2019 provided Region 1 (New England) with a locally themed and accessible cyber exercise. Utilizing a local scenario centered in New Hampshire with a national focus allowed the use of the Emergency Management Assistance Compacts process to ask for assistance from surrounding states. Having a "local" exercise brought in more partners than distant locations would have. Being local allowed the exercise to have participation from National Guard and Reserve units from throughout New England as well as our federal partners from local Region 1 offices. Cyber Yankee 19 utilized a cost effective model versus larger national exercises at remote training centers. Cyber Yankee achieved many similar national level training objectives in a smaller geographic footprint allowing single day (less than 3 hours) travel by ground for most participants. Additionally, as previously stated, operating at the unclassified level ensured maximum participation from military and non-military participants. This enabled more effective sharing and distribution of exercise documents and products. Consideration of this model should be a way ahead for National Guard/Reserve component cyber exercises. A regional model incorporates all key aspects of an exercise at a fraction of the cost of a national event. Cyber Yankee 15-19 proves that centrally funded exercise dollars for regional exercises result in a high return on investment.

APPENDIX A: ACRONYMS

Table B.1: *Acronyms*

Acronym	Meaning
AAR	After Action Report
AAR/IP	After Action Report/Improvement Plan
APAN	All Partners Access Network
ASPR	Assistant Secretary for Preparedness and Response
BCP	Business Continuity Plan
BTFM	Blue Team Field Manual
CNDT	Computer (Cyber) Network Defense Team
CPT	Cyber Protection Team
COOP	Continuity of Operations Plan
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DoS	Denial of Service
DRP	Disaster Response Plan
EOP	Emergency Operations Plan
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GUI	Graphic User Interface
HVA	Hazard Vulnerability Analysis
ICS	Incident Command System
IT	Information Technology
MOU	Memorandum of Understanding
NRF	National Response Framework
POC	Point of Contact
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SQL	Standard Query Language
TCL	Target Capabilities List
TTX	Tabletop Exercise