OPERATIONS ORDERS (OPORDs)

OPORD 1: OPERATION DIGITAL SHIELD

CLASSIFICATION: UNCLASSIFIED//FOR TRAINING USE ONLY
EXERCISE OPORD 001-25
FROM: 25th Cyber Defense Squadron
DTG: 170800ZJUL25

1. SITUATION

a. Enemy Forces: EXERCISE - APT group "Red Phoenix" assessed as highly capable with focus on reconnaissance and lateral movement. Likely objectives include intelligence gathering and system disruption.

b. Friendly Forces: 25th Cyber Defense Squadron with 45 personnel organized into three teams. Supported by regional CERT and FBI cyber division (EXERCISE).

c. Environment: EXERCISE scenario in simulated contested cyber environment with elevated threat levels.

2. MISSION

25th Cyber Defense Squadron conducts defensive cyber operations from 171200Z to 182400Z JUL 25 to detect, analyze, and neutralize simulated APT activity against Blue Force networks in order to maintain operational security and network integrity during EXERCISE.

3. EXECUTION

a. Concept of Operations: Three-phase defensive operation focusing on detection, analysis, and response to simulated threats.

Phase I (1200-1800Z): Enhanced monitoring and threat hunting **Phase II (1800-0600Z):** Active threat engagement and mitigation
Phase III (0600-2400Z): Recovery and lessons learned

b. Tasks to Subordinate Units:

- **Cyber Defense Team Alpha:** Conduct perimeter monitoring using SIEM systems. Report all anomalies within 15 minutes.
- **Cyber Defense Team Bravo:** Execute threat hunting operations focusing on lateral movement indicators.

- **Cyber Defense Team Charlie:** Maintain incident response capability with 30-minute response time.

c. Coordinating Instructions:

- ROE: Defensive measures only during EXERCISE
- All actions require team leader approval
- Maintain detailed logs for after-action review

4. SERVICE SUPPORT

a. Logistics: 24-hour SOC operations with shift changes at 0800, 1600, and 0000.

b. Personnel: Medical support on-site. Backup personnel on 2-hour recall.

c. Miscellaneous: Catering for extended operations. Exercise safety officer assigned.

5. COMMAND AND SIGNAL

a. Command: Squadron commander retains operational control. Deputy commander serves as alternate.

b. Signal: Primary communications via secure chat. Backup through encrypted phone. Emergency procedures per SOP.

ACKNOWLEDGE RECEIPT AND CONFIRM READY STATUS