2. AFCYBER Weapons Systems

2.1 Overview & 2.2 Capabilities

Cyberspace Vulnerability Assessment/Hunter

Mission: The Cyberspace Vulnerability Assessment/Hunter (CVA/H) weapon system executes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and Hunter missions on Air Force and Department of Defense networks and systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. The weapon system can perform defensive sorties world-wide via remote or on-site access.

The CVA/H weapon system is operated by six active duty units located at Joint Base San Antonio-Lackland, Texas, and Scott AFB, Ill. Additionally, twelve Air National Guard units operate the weapon system at various locations across the United States. The Air Force Reserve operates a classic associate unit at Scott AFB.

Background: The CVA/H was developed by the former Air Force Information Operations Center, fielded to the then-688th Information Operations Wing in 2009 and officially designated a weapon system by the Chief of Staff of the Air Force in March 2013. Historically, vulnerability assessments were instrumental to mission assurance during Operations Enduring Freedom and Iraqi Freedom. As the complexity of threats to information systems grew and their impact to operations expanded, CVA/H was developed to increase defensive capability. CVA/H continues to provide mission assurance to our most important systems. Additionally, CVA/H now provides the ability to hunt adversaries in our networks and systems.

The Hunter mission grew out of the change in defensive cyber strategy from "attempt to defend the whole network" to "mission assurance on the network," and provides an enabling capability to implement a robust defense-in-depth strategy. CVA/H has been employed in real-world operations since November 2010. Air Force Space Command declared CVA/H initially operational capable in June 2013 and fully operational capable in February 2016.

Features: The CVA/H weapon system is designed to identify vulnerabilities and provide commanders with a comprehensive assessment of the risk of existing vulnerabilities on critical mission networks. It is functionally divided into a mobile platform used by operators to conduct missions on-site or remotely; a deployable sensor platform to gather and analyze data; and a garrison platform which provides the connectivity needed for remote operations as well as advanced analysis, testing, training, and archiving capabilities. Additionally, the Hunter mission focuses on the capability to find, fix, track, target, engage and assess the advanced persistent threat.

During active engagements, the CVA/H weapon system, in concert with other friendly network defense forces, provides Air Forces Cyber and combatant commanders a mobile precision protection capability to identify, pursue and mitigate cyberspace threats.

The CVA/H weapon system can be armed with a variety of modular capability payloads optimized for specific defensive missions and designed to achieve specific effects in cyberspace. Each CVA/H crew is capable of conducting a range of assessments, to include: vulnerability, compliance and penetration testing, along with analysis and characterization of data derived from these assessments. The weapon

system payloads consist of commercial-off-the-shelf and government-off-the-shelf hardware and software, to include Linux and Windows operating systems loaded with customized vulnerability assessment tools.

General Characteristics

Primary Function: Conduct defensive cyber operations to identify and counter advanced persistent threats to critical capabilities identified by combatant commanders and U.S. Cyber Command.

Crew Positions: One cyberspace crew commander, one to four cyberspace operators and one to four cyberspace analysts. All mission crews are supported by mission support personnel.

Inventory: 30

Major Command: Air Combat Command, Joint Base Langley-Eustis, Va.

Numbered Air Force: 16th Air Force/AFCYBER, JBSA-Lackland, Texas

Cyberspace Defense Analysis

Mission: The Cyberspace Defense Analysis (CDA) weapon system provides operational effects designed to protect and defend critical Air Force data at the nexus of adversarial threats, Air Force priorities and key missions and user behavior on Air Force networks. CDA conducts operations in concert with Air Force Cyberspace Defense, Air Force Intranet Control, Cyberspace Vulnerability Assessment/Hunter, Cyberspace Command and Control Mission System, and Cyberspace Security Control System weapon systems. CDA conducts defensive cyberspace operations by monitoring, collecting, analyzing, and reporting on sensitive information released from friendly unclassified systems, such as computer networks, telephones, email and Air Force websites. CDA is vital to identifying operations security disclosures and is the primary system assigned to provide operations security, communications security and unintentional and intentional insider threat monitoring for all Air Force operations, missions and functions; focusing on data loss prevention and information damage assessments.

CDA is operated by the 68th Network Warfare Squadron (active duty) at Joint Base San Antonio-Lackland, Texas, as well as the 860th Network Warfare Flight and 960th NWF (Air Force Reserve) at Offutt Air Force Base, Neb.

Background: This weapon system evolved from OPSEC programs designed to identify vulnerabilities for commanders in the field. It was officially designated by Chief of Staff of the Air Force in March 2013.

Features: CDA has two variants, both designed to monitor, collect, analyze and report information transmitted via unsecure telecommunications systems to determine whether sensitive or classified information is being transmitted. Compromises are reported to field commanders, OPSEC monitors or others to determine potential impacts and operational adjustments. The second variant currently provides additional functionality for conducting information damage assessment based on network intrusions, and assessing of unclassified Air Force websites. The second variant is only operated by the 68th NWS.

The CDA weapon system provides monitoring and/or assessment in six sub-discipline areas:

1. Telephony: Monitoring and assessing unclassified Air Force voice networks.

2. Radio frequency: monitoring and assessing Air Force communications within the VHF, UHF, FM, HF and SHF frequency bands (mobile phones, land mobile radios, wireless local area networks).

3. Email: Monitoring and assessing unclassified Air Force email traffic traversing the Air Force network.

4. Internet based capabilities: Monitoring and assessing information that originates within the AFNet that is posted to publicly accessible websites not owned, operated, or controlled by the Department of Defense or federal government.

5. Cyberspace operational risk assessment: Assessing data compromised through AFNet intrusions with the objective of determining the associated impact to operations resulting from that data loss. This sub-discipline is in the second variant.

6. Web risk assessment: Assessing information posted on unclassified Air Force-owned, -leased, or -operated public and private web sites in order to minimize exploitation of Air Force information by potential adversaries that can negatively impact Air Force and joint operations. This sub-discipline is in the second variant.

General characteristics

Active indicator monitoring: Preventing unauthorized access to or attacks on Air Force-owned, -leased or -operated systems or networks. Air Forces Cyber commander, through the 624th Operations Center, will task CDA units to search for information vulnerabilities that, if intercepted by an adversary, would facilitate unauthorized access to the Air Force Information Network or increase the effectiveness of adversary cyberspace operations.

Primary Function: Support OPSEC and conduct defensive cyberspace operations by assessing unsecure Air Force communications.

Crew Positions: One cyberspace operations controller and three cyberspace defense analysts. Multiple crews are on duty at any time. All mission crews are supported by mission support personnel.

Inventory: Three

Major Command: Air Combat Command, Joint Base Langley-Eustis, Va.

Numbered Air Force: 16th Air Force/Air Forces Cyber, JBSA-Lackland, Texas

Cyber Command and Control Mission System

Mission: The Cyber Command and Control Mission System (C3MS) weapon system synchronizes other Air Force cyber weapon systems to produce operational-level effects in support of combatant commanders worldwide.

C3MS provides operational level command and control (C2) and situational awareness of Air Force cyberspace forces, networks and mission systems. C3MS enables the 24th Air Force/Air Forces Cyber/Joint Force Headquarters-Cyber commander to develop and disseminate cyber strategies and plans, then execute and assess these plans in support of Air Force and Joint warfighters.

The C3MS weapon system is operated by the 624th Operations Center (active duty) and 854th Combat Operations Squadron (Air Force Reserve) at Joint Base San Antonio-Lackland, Texas, and the 119th Cyber Operations Squadron (Air National Guard) at McGhee Tyson ANG Base, Tenn.

Background: C3MS evolved from the legacy Air Force Network Operations Security Center concept, personnel and equipment. With the activation of U.S. Cyber Command and 24th AF, senior leaders recognized the need for an operational-level cyber C2 capability. C3MS was officially designated by Chief of Staff of the Air Force in March 2013 and initial operating capability was declared July 30, 2014.

Features: C3MS is the single Air Force weapon system providing overarching 24/7 situational awareness, management and control of the Air Force portion of the cyberspace domain. It ensures unfettered access, mission assurance, and joint warfighter use of networks and information processing systems to accomplish worldwide operations. The weapon system has five major sub components:

1. Situational Awareness: Producing a common operational picture by fusing data from various sensors, databases, weapon systems and other sources to gain and maintain awareness of friendly, neutral and threat activities that impact joint forces and the Air Force.

2. Intelligence, Surveillance and Reconnaissance products: Enabling the integration of cyberspace indications and warning, analysis and other actionable intelligence products into overall situational awareness, planning and execution.

3. Planning: Leveraging situational awareness to develop long- and short-term plans, tailored strategy, courses of action, and shape execution of Offensive Cyberspace Operations, Defensive Cyberspace Operations and DoD Information Network Operations.

4. Execution: Leveraging plans to generate and track various cyberspace tasking orders to employ assigned and attached forces in support of OCO, DCO and DoDIN Ops.

5. Integration with other C2 nodes: Providing the ability to integrate Air Force-generated cyber effects with AFCYBER lines of effort, USCYBERCOM and other C2 nodes.

General Characteristics

Primary Function: Operational-level cyber C2 and situational awareness.

Crew Positions: Thirteen unique positions consisting of a senior duty officer, deputy senior duty officer, defensive cyberspace watch officer, offensive cyberspace watch officer, DoDIN Ops watch officer, three DCO controllers, three OCO controllers, three DoDIN Ops controllers, cyberspace effects planner, cyberspace operations strategist, cyberspace intelligence analyst, cyberspace operations assessment analyst, and cyberspace operations reporting cell analyst. All mission crews are supported by mission support personnel.

Inventory: Three

Major Command: Air Combat Command, Joint Base Langley-Eustis, Va.

Numbered Air Force: 16th AF/AFCYBER, JBSA-Lackland, Texas

Air Force Intranet Control

Mission: The Air Force Intranet Control (AFINC) weapon system is the top-level boundary and entry point into the Air Force Information Network, and controls the flow of all external and inter-base traffic through standard, centrally managed gateways.

AFINC consists of 16 gateway suites and two integrated management suites, and is operated by the 26th Network Operations Squadron at Gunter Annex, Montgomery, Ala.

Background: AFINC replaces and consolidates regionally managed disparate Air Force networks into a centrally managed point of access for traffic through the Air Force network. AFINC delivers network-centric services, enables core services and provides greater agility to take defensive actions across the network. AFINC was officially designated by Chief of Staff of the Air Force in March 2013.

Features: AFINC integrates network operations and network defense via four sub-discipline areas:

1. Defense-in-depth: Delivering enterprise-wide layered approach by integrating the gateway and boundary devices to provide increased network resiliency and mission assurance.

2. Proactive defense: Conducting continuous monitoring of AFNet traffic for response time, throughput and performance, to ensure timely delivery of critical information.

3. Network standardization: Creating and maintaining standards and policies to protect networks, systems and databases, and reduce maintenance complexity, down-time, costs and training requirements.

4. Situational awareness: Delivering network data flow, traffic patterns, utilization rates, and in-depth research of historical traffic for anomaly resolution.

General Characteristics

Primary Function: Operates the global-level entry points for the AFIN and the primary interface between each base and the Internet.

Crew Positions: One crew commander, one deputy crew commander, one cyberspace operations crew chief, two operations controllers, two cyberspace operators and three event controllers. All mission crews are supported by mission support personnel.

Inventory: One

Major Command: Air Combat Command, Joint Base Langley-Eustis, Va.

Numbered Air Force: 16th Air Force/Air Forces Cyber, Joint Base San Antonio-Lackland, Texas

Air Force Cyberspace Defense

Mission: The Air Force Cyberspace Defense (ACD) weapon system is designed to prevent, detect, respond to, and provide forensics of intrusions into unclassified and classified networks. This weapon system supports the Air Force Computer Emergency Response Team in fulfilling their responsibilities.

ACD is operated by the 33rd Network Warfare Squadron and 426th NWS (Air Force Reserve), at Joint Base San Antonio-Lackland, Texas, as well as the 102nd NWS (Air National Guard) at Quonset ANG Base, R.I.

Background: ACD evolved from the Air Force Computer Response Team. The AFCERT's primary responsibility was coordination of the former Air Force Information Warfare Center technical resources to assess, analyze, and mitigate computer security incidents and vulnerabilities. ACD was officially designated by the Chief of Staff of the Air Force in March 2013.

Features: ACD provides continuous monitoring and defense of Air Force unclassified and classified networks. ACD operates in four sub-discipline areas:

1. Incident prevention: Protecting Air Force networks against new and existing malicious logic by assessing and mitigating known software and hardware vulnerabilities.

2. Incident detection: Monitoring classified/unclassified Air Force networks, identifying and researching anomalous activity to determine problems and threats to networks, and monitoring real-time alerts generated from network sensors. The system also performs in-depth, historical traffic research reported through sensors.

3. Incident response: Determining the extent of intrusions, developing courses of action required to mitigate threats, and determining and executing response actions. The operational crew interfaces with law enforcement during malicious logic related incidents.

4. Computer forensics: Conducting in-depth analysis to determine threats from identified incidents and suspicious activities, then assessing damage. Supporting incident response process, capturing the full impact of various exploits and reverse engineering code to determine the impact to the network/system.

General Characteristics

Primary Function: Defensive cyberspace operations to prevent, detect and respond to network intrusions.

Crew Positions: One cyberspace crew commander, one deputy crew commander, one cyberspace operations controller, and multiple cyberspace analysts. All mission crews are supported by mission support personnel.

Inventory: Two

Major Command: Air Combat Command, Joint Base Langley-Eustis, Va.

Numbered Air Force: 16th Air Force/Air Forces Cyber, JBSA-Lackland, Texas

Cyber Security and Control System

Mission: The Cyber Security and Control System (CSCS) weapon system is designed to provide 24/7 network operations and management functions and enable key enterprise services within Air Force unclassified and classified networks. This system also supports defensive operations within those Air Force networks.

CSCS is operated by the 83rd Network Operations Squadron (active duty) and 860th NOS (Air Force Reserve) at Langley Air Force Base, Va.; 561st NOS (AD) and 960th NOS (AFR) at Peterson AFB, Colo.; and 299th Network Operations Security Squadron (Air National Guard) at McConnell AFB, Kan. Support is also provided from the 690th Cyberspace Operations Squadron (AD) at Joint Base Pearl Harbor-Hickam, Hawaii, and 691st COS (AD) Ramstein Air Base, Germany. Additional support is received from 690th Intelligence Support Squadron (AD) and 690th Network Support Squadron (AD) at Joint Base San Antonio-Lackland, Texas.

Background: CSCS resulted from an operational initiative to consolidate numerous MAJCOM-specific stove-piped networks into a centrally managed and controlled network under three Integrated Network Operations and Security Centers. This concept evolved to include enterprise services and storage functions under Enterprise Service Units and Area Processing Centers. In 2007, the Air Force established two active duty NOSs to provide these functions. The ANG NOSS provides the same functions for ANG bases and units. CSCS was officially designated by Chief of Staff of the Air Force in March 2013.

Features: CSCS includes the I-NOSC, ESU, APC and Regional Data Centers functions. CSCS performs network operations and fault resolution activities to maintain operational networks. CSCS crews monitor, assess and respond to real-time network events; identify and characterize anomalous activity; and take appropriate response actions when directed by higher headquarters. The system supports real-time filtering of network traffic into/out of Air Force base-level enclaves and blocks suspicious software. CSCS crews continuously coordinate with base-level network control centers and communications focal points to resolve network issues. Additional key capabilities include vulnerability identification and remediation, as well as control and security of network traffic entering and exiting Air Force base-level network enclaves. CSCS also provides Air Force enterprise services to include messaging and collaboration services, storage, and controlled environments for hosting network-based systems supporting Air Force missions.

General Characteristics

Primary Function: Air Force information network operations and proactive defense.

Crew Positions: One cyberspace crew commander, one cyberspace operations controller, an operations flight crew (conducting boundary, infrastructure, network defense, network focal point and vulnerability management functions) and an ESU flight crew (providing messaging and collaboration, directory and authentication services, storage and virtualization management and monitoring management). All mission crews are supported by mission support personnel.

Inventory: Three

Major Command: Air Combat Command, Joint Base Langley-Eustis, Va.

Numbered Air Force: 16th Air Force/Air Forces Cyber, JBSA-Lackland, Texas