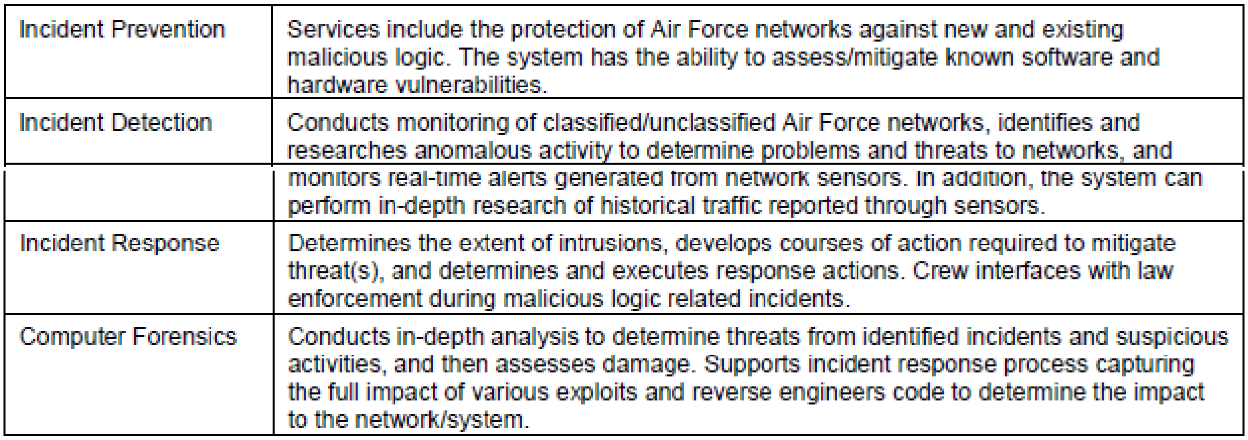
Security Tools

Proficiency Code: B

Air Force Cyberspace Defense Weapon System

The Air Force Cyberspace Defense (ACD) allows for defensive cyber operations to prevent, detect, respond to, and provide forensics of intrusions into unclassified and classified networks. The 33rd Network Warfare Squadron (NWS) located at Joint Base San Antonio Lackland TX, and the ANG's 102d NWS located at Quonset ANGB Rhode Island, and falls under the 24th AF operate the ACD. ACD provides continuous monitoring and defense of AF unclassified and classified networks. The ACD weapon system operates in four sub-discipline areas displayed in the table.



Incident Prevention	Services include the protection of Air Force networks against new and existing malicious logic. The system has the ability to assess/mitigate known software and hardware vulnerabilities.
Incident Detection	Conducts monitoring of classified/unclassified Air Force networks, identifies and researches anomalous activity to determine problems and threats to networks, and monitors real-time alerts generated from network sensors. In addition, the system can perform in-depth research of historical traffic reported through sensors.
Incident Response	Determines the extent of intrusions, develops courses of action required to mitigate threat(s), and determines and executes response actions. Crew interfaces with law enforcement during malicious logic related incidents.
Computer Forensics	Conducts in-depth analysis to determine threats from identified incidents and suspicious activities, and then assesses damage. Supports incident response process capturing the full impact of various exploits and reverse engineers code to determine the impact to the network/system.

The ACD weapon system evolved from the Air Force Computer Emergency Response Team (AFCERT). 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.

Air Force Cyber Security and Control System Weapon System

The Air Force Cyber Security and Control System (CSCS) weapon system provides 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. Two active duty (AD) Network Operations Squadrons (NOS), one ANG Network Operations Security Squadron (NOSS) and two Air Force Reserve Command (AFRC) Associate NOSs aligned with the AD squadrons operate the CSCS. Each unit operationally falls under the 24th AF and assigned to AFSPC.

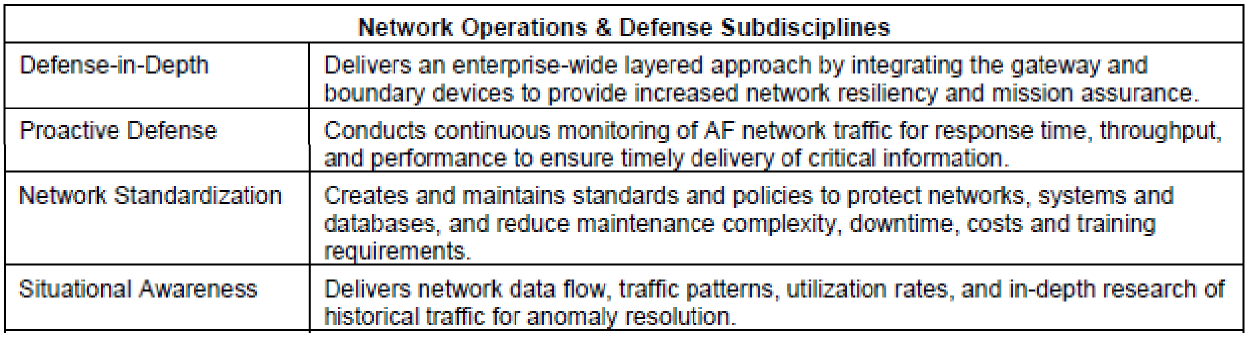
The CSCS weapon system includes the Integrate Network Operations Security Center (I-NOSC), Enterprise Service Unit (ESU) and Area Processing Center (APC) functions. CSCS performs network operations and fault resolution activities designed to maintain operational networks. CSCS crews monitor, assess and 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 in and out of Air Force base-level enclaves and blocks suspicious software. CSCS crews continuously coordinate with base level network control centers (NCC) and communications focal points (CFP) 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 AF enterprise services to include messaging and collaboration services, storage, and controlled environments for hosting network-based systems supporting Air Force missions.

The CSCS resulted from an operational initiative to consolidate numerous MAJCOM-specific stove-piped networks into a centrally managed and controlled network under three I-NOSCs. This concept evolved to include enterprise services and storage functions under ESUs and APCs.

Air Force Intranet Control Weapon System

The Air Force Intranet Control (AFINC) weapon system is the top-level boundary and entry point into the AFIN, and controls the flow of all external and inter-base traffic through standard, centrally managed gateways. The AFINC weapon system consists of 16 Gateway Suites and two Integrated Management Suites, and is operated by the 26th NOS located at Gunter Annex, Montgomery, AL, and falls under the 24th AF, within AFSPC.

The AFINC weapon system integrates network operations and network defense via four sub-discipline areas.



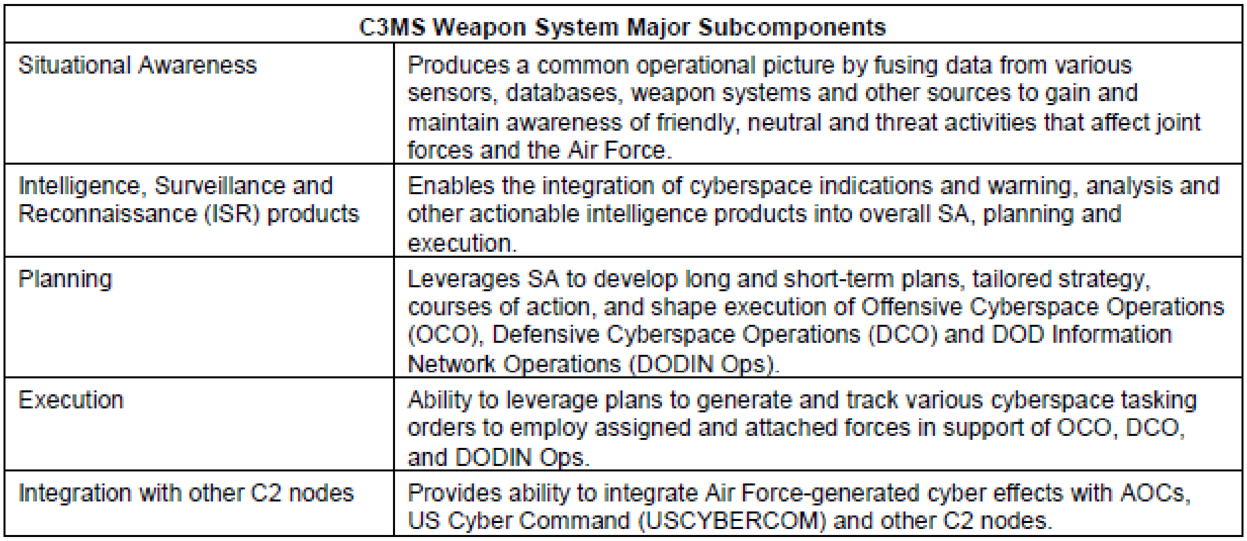
Network Operations & Defense Subdisciplines	
Defense-in-Depth	Delivers an enterprise-wide layered approach by integrating the gateway and boundary devices to provide increased network resiliency and mission assurance.
Proactive Defense	Conducts continuous monitoring of AF network traffic for response time, throughput, and performance to ensure timely delivery of critical information.
Network Standardization	Creates and maintains standards and policies to protect networks, systems and databases, and reduce maintenance complexity, downtime, costs and training requirements.
Situational Awareness	Delivers network data flow, traffic patterns, utilization rates, and in-depth research of historical traffic for anomaly resolution.

The AFINC weapon system replaces and consolidates regionally managed disparate Air Force networks into a centrally managed point of access for traffic through the Air Force network. The AFINC weapon system delivers network centric services, enables core services and provides greater agility to take defensive actions across the network.

Cyber Command and Control Mission System Weapon System

The U.S. Air Force has mastered the ability to apply global reach, power and vigilance across the domains of air and space. The AF applies these same precepts in the cyberspace domain as part of its mission to fly, fight and win in air, space and cyberspace. The Cyber Command and Control Mission System (C3MS) weapon system enables this mission by synchronizing other AF cyber weapon systems to produce operational level effects in support of combatant commanders worldwide. C3MS provides operational level C2 and situational awareness (SA) of AF cyber forces, networks and mission systems. C3MS enables the 24th Air Force Commander (24 AF/CC) to develop and disseminate cyber strategies and plans, then execute and assess these plans in support of AF and Joint warfighters. The C3MS weapon system is operated by the 624th Operations Center (624 OC) at Joint Base San Antonio Lackland, TX, and falls under the 24th AF under AFSPC.

The C3MS weapon system is the single AF weapon system providing overarching 24/7/365 awareness, management and control of the AF portion of the cyberspace domain. C3MS 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 subcomponents as displayed in the table.



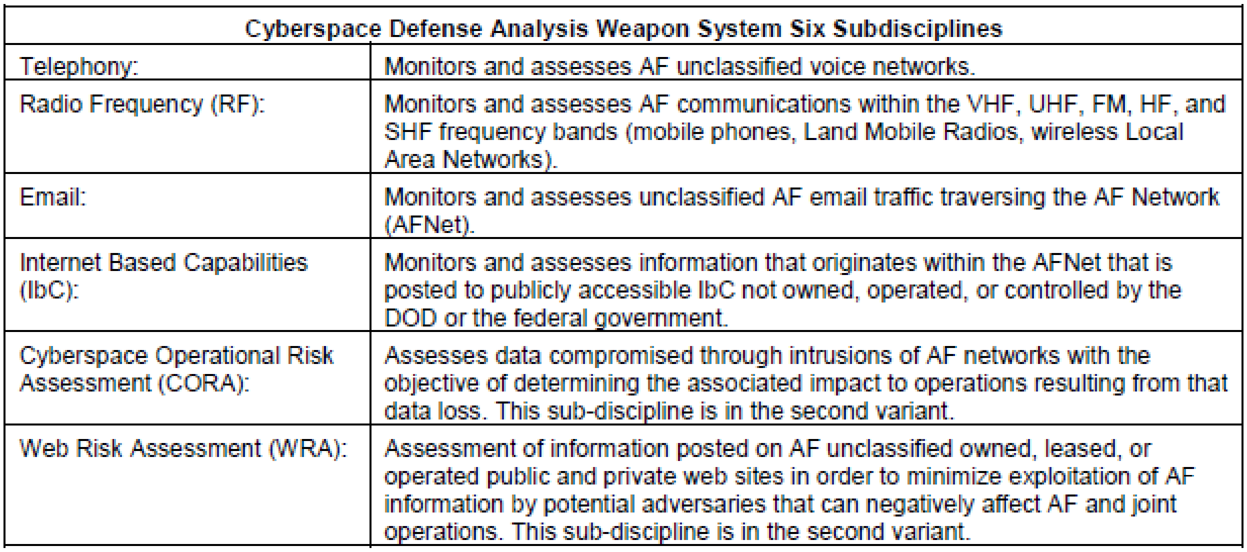
C3MS Weapon System Major Subcomponents	
Situational Awareness	Produces a common operational picture by fusing data from various sensors, databases, weapon systems and other sources to gain and maintain awareness of friendly, neutral and threat activities that affect joint forces and the Air Force.
Intelligence, Surveillance and Reconnaissance (ISR) products	Enables the integration of cyberspace indications and warning, analysis and other actionable intelligence products into overall SA, planning and execution.
Planning	Leverages SA to develop long and short-term plans, tailored strategy, courses of action, and shape execution of Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO) and DOD Information Network Operations (DODIN Ops).
Execution	Ability to leverage plans to generate and track various cyberspace tasking orders to employ assigned and attached forces in support of OCO, DCO, and DODIN Ops.
Integration with other C2 nodes	Provides ability to integrate Air Force-generated cyber effects with AOCs, US Cyber Command (USCYBERCOM) and other C2 nodes.

The C3MS weapon system evolved from the legacy AF Network Operations Security Center concept, personnel, and equipment. With the activation of USCYBERCOM and 24th AF, senior leaders recognized the need for an operational level Cyber C2 capability.

Cyberspace Defense Analysis Weapon System

The Air Force Cyberspace Defense Analysis (CDA) weapon system 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 USAF Websites. CDA is vital to identifying operations security (OPSEC) disclosures. Three active duty units and two reserve units assigned to the 24th AF within AFSPC operate the CDA weapon system.

The CDA weapon system has two variants, which monitor, collect, analyze and report on information transmitted via unsecured telecommunications systems to determine whether sensitive or classified information is transmitting. Data 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 assessment of AF unclassified web sites. The 68 NWS is the only unit that operates the second variant. The CDA weapon system provides monitoring and/or assessment in six sub-discipline areas as displayed in the table.



Cyberspace Defense Analysis Weapon System Six Subdisciplines	
Telephony:	Monitors and assesses AF unclassified voice networks.
Radio Frequency (RF):	Monitors and assesses AF communications within the VHF, UHF, FM, HF, and SHF frequency bands (mobile phones, Land Mobile Radios, wireless Local Area Networks).
Email:	Monitors and assesses unclassified AF email traffic traversing the AF Network (AFNet).
Internet Based Capabilities (IbC):	Monitors and assesses information that originates within the AFNet that is posted to publicly accessible IbC not owned, operated, or controlled by the DOD or the federal government.
Cyberspace Operational Risk Assessment (CORA):	Assesses data compromised through intrusions of AF networks with the objective of determining the associated impact to operations resulting from that data loss. This sub-discipline is in the second variant.
Web Risk Assessment (WRA):	Assessment of information posted on AF unclassified owned, leased, or operated public and private web sites in order to minimize exploitation of AF information by potential adversaries that can negatively affect AF and joint operations. This sub-discipline is in the second variant.

This weapon system grew from OPSEC programs designed to identify vulnerabilities for commanders in the field.

Cyberspace Vulnerability Assessment/Hunter Weapon System

The Air Force Cyberspace Vulnerability Assessment/Hunter (CVA/Hunter) weapon system executes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and Hunter missions on AF and DOD networks & systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. The weapon system can perform defensive sorties worldwide via remote or on-site access. The CVA/Hunter operates under the command of the 24the Air Force within AFSPC.

The CVA/Hunter weapon system identifies vulnerabilities and provides 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 onsite 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. Specifically, the Hunter mission focuses on the capability to find, fix, track, target, engage, and assess (F2T2EA) the advanced persistent threat (APT).

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

The CVA/Hunter weapon system has a variety of modular capability payloads optimized for specific defensive missions and designed to achieve specific effects in cyberspace. Each CVA/Hunter 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 (COTS) and government-off-the-shelf (GOTS) hardware and software, to include Linux and Windows operating systems loaded with customized vulnerability assessment tools.

Historically, vulnerability assessments were instrumental to mission assurance during Operations Enduring Freedom and Iraqi Freedom. CVAs continue to provide this vital capability. Additionally, they now serve as the first phase of hunting operations.

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. November 2010 began CVA/Hunter weapon system employment in real-world operations.