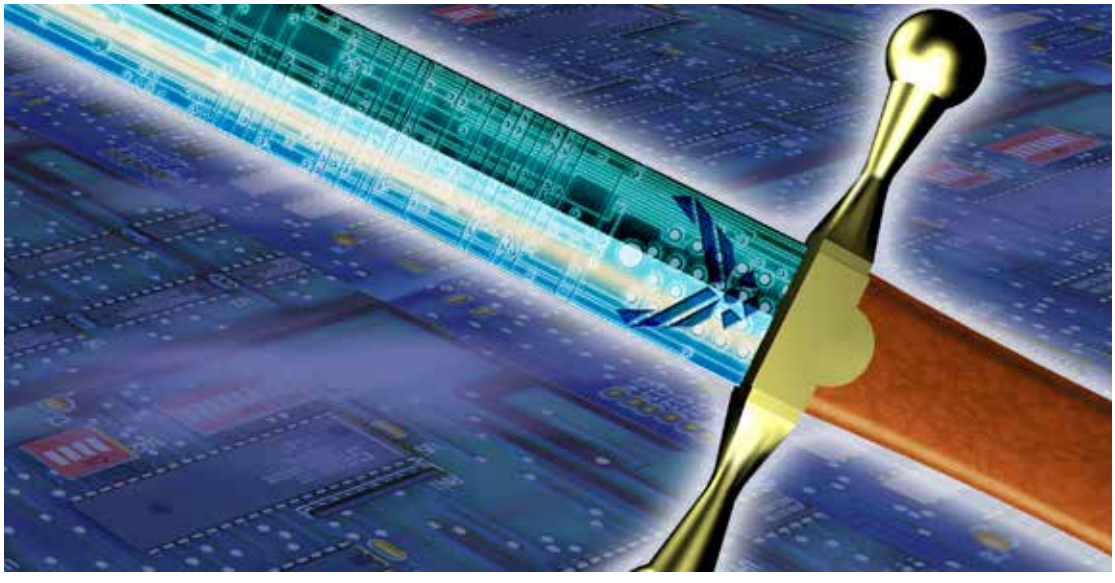
The Importance of Designating Cyberspace Weapon Systems

Brig Gen Robert J. Skinner, USAF



Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines *weapon system* as "a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency."[1] When one thinks of the US Air Force and weapon systems, the B-2 Spirit stealth bomber, F-15E Strike Eagle fighter jet, or F-16 Fighting Falcon aircraft quickly come to mind. Even the Minuteman III missile, the Global Positioning System, or KC-135 Stratotanker air refueling aircraft could become part of the discussion because, after all, the Air Force's mission is to fly, fight, and win in air, space, and cyberspace. These assets, which fall under the air and space umbrella, have served as tried and true weapon systems for many years. The Air Force has now added to the long line of its

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Importance of Designating Cyberspace Weapon Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute,Air & Space Power Journal ,155 N. Twining Street,Maxwell AFB,AL,36112-6026**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**20**	

weapon systems that support cyberspace operations "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." These systems are unique in that they are tied to the newest domain of cyber—"a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2]

On 24 March 2013, the chief of staff of the Air Force approved the official designation of six cyberspace weapon systems under the lead of Air Force Space Command (AFSPC), which is responsible for organizing these systems, equipping units with them, and training individuals to use the systems. The Air Force's provision of global reach, power, and vigilance across the domains of air and space now applies to the cyberspace domain through the designation of the following cyberspace weapon systems:

- Air Force Cyberspace Defense
- Cyberspace Defense Analysis
- Cyberspace Vulnerability Assessment / Hunter
- Air Force Intranet Control
- Air Force Cyber Security and Control System
- Cyber Command and Control Mission System

Although the names may imply some duplication of effort with respect to these capabilities, the personnel and equipment that comprise these systems perform unique missions and complement each other. All of them focus on providing and securing cyberspace as a mission enabler and protecting critical information while defending our networks from attack. Any consideration of the capabilities of these weapon systems would benefit from comparing this suite of cyberspace weapon systems to the Air Force's military airlift weapon systems (the C-5, C-17, C-130, etc.), each of which contributes uniquely to

the overall air mobility mission. Just as clear distinctions exist among these platforms, based upon the operational capabilities required, so do the cyberspace weapon systems differ from each other. The systems may have overlapping mission areas, but they are complementary in much the same way as our airlift platforms—they offer comprehensive capabilities.

Revelations of Chinese activities on our networks, as outlined earlier this year in the Mandiant Company's report titled *Advanced Persistent Threat (APT) 1: Exposing One of China's Cyber Espionage Units*, emphasize the urgent need for the Air Force and the nation to develop capabilities to defend this critical domain and thereby ensure information superiority. The report illustrates the persistent threat, noting that "the details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them. . . . Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors." The Mandiant report on APT 1 highlights only one of more than 20 APT groups based in China, tracking this single group to cyber attacks on nearly 150 victims over seven years with hundreds of terabytes of data exfiltrated.[3] Clearly, though, this discussion does not confine itself to any particular adversary. Many aggressors inhabit the cyberspace domain, and the executor of these activities ranges from an individual in the basement of his house, to groups of individuals working as teams, to nation-states. Their intentions can also cover a spectrum of activities, including espionage, theft of intellectual capital, organized crime, identity theft, military operations, and so forth.

This article examines each weapon system, highlights its history and unique capabilities, and describes the specific units that operate the system. It then discusses the importance of classifying these capabilities as "weapon systems," illustrating how they directly address the threats we face today. Before doing so, however, the article presents a

stage-setting vignette to establish an understanding of weapon system capabilities and their employment against an adversary.

Assume that you are a government civilian sitting at your desk at a major command headquarters when you receive an e-mail concerning sequestration and a potential furlough. Included in the e-mail is a link to a website for more information. You attempt to open the link but receive an error message. You try again with the same result. You then resume work on your tasks. Unknown to you, the link has directed you to a malicious web server that downloaded malware enabling an adversary to take command of your desktop computer. How could this occur, and why would anyone specifically target you? Actually, it was not difficult. Remember the conference you attended a few months ago, before temporary duty became restricted? The adversary lifted your e-mail address from the conference sign-in sheet, also available to the event sponsors. Why you? Adversaries consider your unique expertise and access to valuable information a "target-rich environment." Only one person needs to click on the link to initiate a series of malicious actions. Because the adversary left no hint of a problem on your computer, he now has unfettered access to that unclassified but useful information.

How does the Air Force combat such intrusions? Actually, the best defense for phishing attacks is user education. However, these attacks are becoming more sophisticated and sometimes almost impossible to identify. All of the services have cyberspace units responsible for network defense. In this case, network traffic monitoring tips off the Air Force to the intrusion on your desktop computer. A network operations unit identifies an unusual amount of traffic leaving your base directed to addresses in another country. The unit notifies the 624th Operations Center, including Air Force Office of Special Investigations personnel, and the center begins command and control (C2) and law enforcement efforts to address the event. Cyberspace forensics experts are dispatched to review the situation, not only locating the "infected" equipment but also determining how the adversary accessed the Air Force

system. Cyberspace C2 dispatches cyber operations risk-assessment personnel to survey the situation, determine the exact data exfiltrated, and assess the damage. The Air Force computer emergency response team (AFCERT) examines your base's computers and other hardware to footprint exact infiltration methods, using them to develop (and share) defensive actions specific to the threat and glean any new tactics, techniques, and procedures. The AFCERT pushes patches to all Air Force desktop computers to combat future attempts to employ this technique; it will support your base on further network cleanup and hardening. Now that we have described an attack from 50,000 feet, let us delve deeper into the weapon systems and units that carry out these missions.

Air Force Cyberspace Defense Weapon System

The Air Force Cyberspace Defense (ACD) weapon system prevents, detects, responds to, and provides forensics of intrusions into unclassified and classified networks. Operated by the 33d Network Warfare Squadron (NWS), located at Joint Base San Antonio–Lackland, Texas, and the Air National Guard's 102d NWS, located at Quonset Air National Guard Base, Rhode Island, the ACD weapon system supports the AFCERT in fulfilling its responsibilities. The crews for this weapon system consist of one cyberspace crew commander, one deputy crew commander, one cyberspace operations controller, and 33 cyberspace analysts, all of them supported by additional mission personnel.

The ACD weapon system evolved from the AFCERT, which has primary responsibility for coordinating the former Air Force Information Warfare Center's technical resources to assess, analyze, and mitigate computer security incidents and vulnerabilities. The weapon system offers continuous monitoring and defense of the Air Force's unclassified and classified networks, operating in four subdiscipline areas:

1. incident prevention: protects Air Force networks (AFNet) against new and existing malicious logic; assesses and mitigates known software and hardware vulnerabilities.
2. incident detection: conducts monitoring of classified and unclassified AFNets; identifies and researches anomalous activity to determine problems and threats to networks; monitors real-time alerts generated from network sensors; performs in-depth research of historical traffic reported through sensors.
3. incident response: determines the extent of intrusions; develops courses of action required to mitigate threat(s); determines and executes response actions.
4. computer forensics: conducts in-depth analysis to determine threats from identified incidents and suspicious activities; assesses damage; supports the incident response process, capturing the full impact of various exploits; reverse-engineers code to determine the effect on the network/system.

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, e-mail, and US Air Force websites. CDA is vital to identifying operations security disclosures. The weapon system is operated by three active duty units (68 NWS; 352 NWS; and 352 NWS, Detachment 1) and two Air Force Reserve units (860th Network Warfare Flight and 960th Network Warfare Flight) located at Joint Base San Antonio–Lackland, Texas; Joint Base Pearl Harbor–Hickam Field, Hawaii; Ramstein Air Base, Germany; and Offutt AFB, Nebraska. The crews for this weapon system consist of one cyberspace operations controller and three cyberspace defense analysts. All mission crews receive support from additional mission personnel.

The CDA weapon system's two variants are designed to monitor, collect, analyze, and report on official Air Force information transmitted via unsecured telecommunications systems to determine whether any of it is sensitive or classified. The system reports compromises to field commanders, operations security monitors, or others, as required, to determine potential effects and operational adjustments. The second variant provides additional functionality to conduct information damage assessment based on network intrusions, coupled with an assessment of Air Force unclassified websites. Only the 68 NWS operates the second variant.

The CDA weapon system supplies monitoring and/or assessment in six subdiscipline areas:

1. telephony: monitors and assesses Air Force unclassified voice networks.
2. radio frequency: monitors and assesses Air Force communications within the VHF, UHF, FM, HF, and SHF frequency bands (mobile phones, land mobile radios, and wireless local area networks).
3. e-mail: monitors and assesses unclassified Air Force e-mail traffic traversing the AFNet.
4. Internet-based capabilities: monitor and assess information that originates within the AFNet that is posted to publicly accessible Internet-based capabilities not owned, operated, or controlled by the Department of Defense (DOD) or the federal government.
5. cyberspace operational risk assessment (found within the second variant operated by the 68 NWS): assesses data compromised through intrusions of AFNets with the objective of determining the associated effect on operations resulting from that data loss.
6. web risk assessment (found within the second variant operated by the 68 NWS): assesses information posted on unclassified public and private websites owned, leased, or operated by the Air Force in order to minimize its exploitation by an adversary, diminishing any adverse affect on Air Force and joint operations.

Cyberspace Vulnerability Assessment / Hunter Weapon System

The Air Force Cyberspace Vulnerability Assessment (CVA) / Hunter weapon system executes vulnerability, compliance, defense, and non-technical assessments, best-practice reviews, penetration testing, and hunter missions on Air Force and DOD networks and systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. This weapon system can perform defensive sorties worldwide via remote or on-site access. The CVA/Hunter weapon system is operated by one active duty unit, the 92d Information Operations Squadron, located at Joint Base San Antonio–Lackland, Texas, and one Guard unit, the 262 NWS, located at Joint Base Lewis-McChord, Washington. Additionally, two Guard units are in the process of converting to this mission: the 143d Information Operations Squadron located at Camp Murray, Washington, and the 261 NWS located at Sepulveda Air National Guard Station, California. The crews for this weapon system consist of one cyberspace crew commander, one to four cyberspace operators, and one to four cyberspace analysts. Additional mission personnel support all of the mission crews. Developed by the former Air Force Information Operations Center, the CVA/Hunter weapon system was fielded to the 688th Information Operations Wing in 2009.

Historically, vulnerability assessments proved 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," offering an enabling capability to implement a robust defense-in-depth strategy. CVA/Hunter weapon system prototypes have participated in real-world operations since November 2010. The weapon system attained initial operational capability in June 2013.

Designed to identify vulnerabilities, the CVA/Hunter gives commanders 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 either on site or remotely, a deployable sensor platform to gather and analyze data, and a garrison platform that provides needed connectivity for remote operations as well as advanced analysis, testing, training, and archiving capabilities. Specifically, the hunter mission focuses on finding, fixing, tracking, targeting, engaging, and assessing the advanced, persistent threat.

During active engagements, the CVA/Hunter weapon system, in concert with other friendly network defense forces, provides Twenty-Fourth Air Force / Air Forces Cyber and combatant commanders a mobile precision-protection capability to identify, pursue, and mitigate cyberspace threats. It can be armed with a variety of modular capability payloads optimized for specific defensive missions and designed to produce specific effects in cyberspace. Each CVA/Hunter crew can conduct a range of assessments, including vulnerability, compliance, and penetration testing, along with analysis and characterization of data derived from these assessments. The weapon system's payloads consist of commercial-off-the-shelf and government-off-the-shelf hardware and software, including Linux and Windows operating systems loaded with customized vulnerability-assessment tools.

Air Force Intranet Control Weapon System

The Air Force Intranet Control (AFINC) weapon system is the top-level boundary and entry point into the Air Force Information Network, controlling the flow of all external and interbase traffic through standard, centrally managed gateways. The AFINC weapon system consists of 16 gateway suites and two integrated management suites. Operated by the 26th Network Operations Squadron (NOS) located at Gunter Annex, Montgomery, Alabama, AFINC has crews consisting of one crew commander, one deputy crew commander, one cyberspace

operations crew chief, two operations controllers, two cyberspace operators, and three event controllers, all of them supported by additional mission personnel.

The AFINC weapon system replaces and consolidates regionally managed, disparate AFNets into a centrally managed point of access for traffic through the Air Force Information Network. It delivers network-centric services, enables core services, and offers greater agility to take defensive actions across the network. AFINC integrates network operations and defense via four subdiscipline areas:

1. defense-in-depth: delivers an enterprise-wide layered approach by integrating the gateway and boundary devices to provide increased network resiliency and mission assurance.
2. proactive defense: conducts continuous monitoring of AFNet traffic for response time, throughput, and performance to ensure timely delivery of critical information.
3. network standardization: creates and maintains standards and policies to protect networks, systems, and databases; reduces maintenance complexity, downtime, costs, and training requirements.
4. situational awareness: delivers network data flow, traffic patterns, utilization rates, and in-depth research of historical traffic for anomaly resolution.

Air Force Cyber Security and Control System Weapon System

The Air Force Cyber Security and Control System (CSCS) weapon system provides network operations and management functions around the clock, enabling key enterprise services within the Air Force's unclassified and classified networks. It also supports defensive operations within those AFNets. CSCS is operated by two active duty NOSs, one Air National Guard Network Operations Security Squadron,

and two Air Force Reserve Command Associate NOSs aligned with the active duty squadrons. The 83 NOS and 860 NOS are located at Langley AFB, Virginia; the 561 NOS and 960 NOS at Peterson AFB, Colorado; and the 299th Network Operations Security Squadron at McConnell AFB, Kansas. Crews for this weapon system consist of 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 Enterprise Service Unit (supplying messaging and collaboration, directory and authentication services, storage and virtualization management, and monitoring management). Additional mission personnel support all of the mission crews.

The CSCS resulted from an operational initiative to consolidate numerous major command–specific networks into a centrally managed and controlled network under three integrated network operations and security centers. In 2007 the Air Force established two active duty NOSs to provide these functions. The Air National Guard Network Operations Security Squadron does the same for the Guard's bases and units.

The CSCS weapon system performs network operations and fault-resolution activities designed to maintain operational networks. Its crews monitor, assess, and respond to real-time network events; identify and characterize anomalous activity; and take appropriate responses when directed by higher headquarters. The system supports real-time filtering of network traffic into and 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 offers Air Force enterprise services, including messaging and collaboration, storage, and

controlled environments for hosting network-based systems that support the service's missions.

Cyber Command and Control Mission System Weapon System

The Cyber Command and Control Mission System (C3MS) weapon system enables the Air Force mission by synchronizing the service's other cyber weapon systems to produce operational-level effects in support of combatant commanders worldwide. It provides operational-level C2 and situational awareness of Air Force cyber forces, networks, and mission systems, enabling the Twenty-Fourth Air Force commander to develop and disseminate cyber strategies and plans; the commander can then execute and assess these plans in support of Air Force and joint war fighters. Operated by the 624th Operations Center at Joint Base San Antonio–Lackland, Texas, the C3MS weapon system has crews consisting of a senior duty officer, a deputy senior duty officer, a defensive cyberspace watch officer, an offensive cyberspace watch officer, a DOD information network watch officer, three defensive cyber operations controllers, three offensive cyber operations controllers, three DOD information network operations controllers, a cyberspace effects planner, a cyberspace operations strategist, a cyberspace intelligence analyst, a cyberspace operations assessment analyst, and a cyberspace operations reporting cell analyst. All mission crews are supported by additional mission personnel. The C3MS weapon system evolved from the legacy AFNet operations security center's concept, personnel, and equipment. With the activation of US Cyber Command and Twenty-Fourth Air Force, senior leaders recognized the need for an operational-level cyber C2 capability.

The C3MS is the single Air Force weapon system offering perpetual, overarching awareness, management, and control of the service's portion of the cyberspace domain. It ensures unfettered access, mission assurance, and joint war fighters' use of networks and information-

processing systems to conduct worldwide operations. The weapon system has five major subcomponents:

1. 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.
2. intelligence, surveillance, and reconnaissance (ISR) products: enable the integration of cyberspace indications and warning, analysis, and other actionable intelligence products into overall situational awareness, planning, and execution.
3. planning: leverages situational awareness to develop long- and short-term plans, tailored strategy, courses of action; shapes execution of offensive cyberspace operations, defensive cyberspace operations, and DOD information network operations.
4. execution: leverages plans to generate and track various cyberspace tasking orders to employ assigned and attached forces in support of offensive cyberspace operations, defensive cyberspace operations, and DOD information network operations.
5. integration with other C2 nodes: integrates Air Force–generated cyber effects with air and space operations centers (AOC), US Cyber Command, and other C2 nodes.

Why Cyber Weapon Systems?

If we truly wish to treat cyberspace as an operational domain no different from air, land, sea, or space, then our thinking must evolve from communications as a supporting function to cyber as an operational war-fighting domain. To fly and fight effectively and to win in cyberspace, the Air Force must properly organize, train, and equip its cyber professionals. For many years, AFNet infrastructure and systems grew as a result of multiple communities adding components to suit their individual needs, often with end-of-year funds. Similarly, the

components that now make up these six systems had no lead major command to articulate operational requirements and ensure standardized training as well as the effective management and resourcing of equipment life cycles. Such an inconsistent approach made mission assurance and the defense of critical Air Force and joint missions in cyberspace nearly impossible. Migration to the AFNet has allowed the service to take great strides towards realizing the vision from nearly two decades ago of operationalizing and professionalizing the network. AFSPC championed the effort to identify these six systems' weapon systems and facilitate this move to a more disciplined approach. Formally designating these systems helps ensure proper management and sustainment of equipment life cycles. It also expedites the evolution of Air Force cyber professionals from a communications or information technology mind-set to an operational one replete with mission-qualification training, crew force-management standards, and standardization and evaluation programs (where appropriate) to normalize cyber operations, as is the case with space and missile operations. Furthermore, formally designated weapon systems should help cyber receive the proper manning and programmatic funding necessary to ensure that the Air Force can fly, fight, and win in cyberspace.

The DOD construct for the management and resourcing of air, space, land, and sea superiority occurs via weapon systems. The best way to create and control effects in the cyber domain involves using the same weapon system construct to manage and resource cyber capabilities. Cyber weapon systems offer a path for the Air Force to operationalize, normalize, and ultimately standardize cyber, just as we have with the other war-fighting domains. The Air Force has been charged with securing, operating, and defending its portion of the DOD information networks and with defending Air Force and joint missions in the cyberspace domain. These cyber weapon systems give the Air Force a path to follow in normalizing operations to realize this goal.

The designation of cyber weapon systems created a separate cyber-sustainment funding line in the overall process of sustaining Air Force

weapon systems. By normalizing the funding process, the service has instituted proper long-term planning and programming of sustainment funding, thus enabling more effective and efficient use of these limited resources, as compared to uncoordinated execution of unreliable end-of-year funds—key tenets to guaranteeing standardized configuration management and servicewide (and, where applicable, joint) interoperability. We are already realizing these benefits through the deployment of AFNet, whereby the Air Force enterprise has become easier to defend and the user experience continues to improve through ongoing standardization.

The benefits of designating cyberspace weapon systems are similar to those gained by weapon systems in other domains—it is the standard Air Force mechanism for organizing, training, equipping, and presenting mission capabilities. The weapon system construct allows the service to manage operational capabilities in a formalized approach and assure their standardization, sustainment, and availability to combatant commanders. When AFSPC personnel compared the air and space domains' normalization processes, they found that only weapon system designation delivered the desired end state. Such systems may not always be ideally resourced, but they certainly receive better support than they would without designations.

Furthermore, designating cyberspace weapon systems directly supports AFSPC's role as cyber core function lead integrator, enabling the command to meet responsibilities listed in Air Force Policy Directive 10-9 and facilitating standardization across cyberspace platforms.[4] Designating these weapon systems is also critical to providing tactical units with the resources and training they need to operate in a normalized capacity. The core of cross-domain integration lies in the ability to leverage capabilities from different domains to create unique and decisive effects—if adequately resourced. Such designations will support proper evolution of the cyberspace domain and its relationship with the other operational domains—a critically important point because in modern warfare, cyberspace interconnects all domains. All of these ef-

forts to normalize and operationalize cyberspace operations and missions drive the Air Force towards the joint information environment (JIE) construct, standards, and processes. As the DOD, US Cyber Command, and services implement the JIE, they are also standing up cyber mission teams to support national, combatant command, and service-specific cyber requirements. Designating these capabilities as weapon systems allows these teams to better support national and joint missions in, through, and from cyberspace.

Unique Challenges of the Cyber Domain

The air, land, sea, and space domains are natural areas—we didn't have to build them, as we did the tools to leverage those domains. Although none of the natural domains demands any maintenance, cyberspace predominantly exists within the equipment and devices designed, built, and configured by humans, requiring constant maintenance as equipment becomes outdated or worn out. Additionally, the way we construct cyberspace has a direct effect on our ability to operate and defend the domain. This aspect makes cyberspace unique in that its operation is just as important as its defense. We must constantly feed and care for the domain as well as innovate to stay ahead of or, preferably, drive the technology curve.

Defending cyber also presents its own challenges since an adversary can launch a cyber attack virtually without warning from any location on the globe. In the case of intercontinental ballistic missiles, we at least have sensors that detect the launch; thus, depending on the location of the launch, our forces have some modicum of warning and can respond. In cyberspace, attacks can occur without warning or time to craft and execute responses. The Air Force must develop capabilities to detect such attacks, prevent them if possible, and respond accordingly if required, just as it does in all other war-fighting domains. We must also develop the tools to leverage cyberspace for our own benefit. In reality, we may never be able to defend our networks completely—to do so would likely require so much security that we lose the force-

multiplying benefits that cyberspace offers to all of our missions. If we keep all adversaries out, most likely we will keep ourselves locked in. The key lies in finding a balance so that we effectively defend our networks and the missions that rely on them from attack yet leverage cyberspace for the benefit it offers those same missions.

Moreover, cyberspace is critical to Air Force and joint operations in the other war-fighting domains. Practically everything we do in warfare these days relies on cyberspace, be it providing telemetry to satellites and missiles or controlling our military forces in Afghanistan—we depend upon the cyber domain to execute operations in all of the other domains.

Designating cyberspace weapon systems calls for a tremendous resource commitment to meet the standards of air and space weapon systems. Operating to this higher benchmark requires corresponding funding and manpower greater than the cyberspace domain received as a simple communications or information technology support function. However, failure to make these commitments could prove devastating to future operations throughout every other domain. The operationalization of cyberspace is more than just a way for AFSPC to properly organize, train, and equip cyberspace forces—it is the logical evolution of cyberspace to a true war-fighting domain and a critical enabler of all other war-fighting operations.

Air and Space Operating Center Example

In the late 1990s, the Air Force designated the Falconer AOC a weapon system with little or no formal acquisition, sustainment, or requirements rigor to back it up. Basically, the chief of staff just made it a "go do." The operations community found itself backing into the requirements in much the same way we do today with our cyberspace systems. By declaring the AOC a weapon system, the Air Force sought to normalize what was basically a homegrown "county option" collection of equipment and personnel that varied from one numbered air

force to another. This thinking held that a designated weapon system would result in better training for AOC crews, better defense of the program in the program objective memorandum process, and some protection of the numbered air force's staff manpower from poaching to fill AOC billets.

In reality, the AOC funding line has suffered numerous cuts, the equipment baseline has always been problematic in terms of sustainment and modernization, and AOC manpower has remained subject to several efficiency drills, ultimately shrinking the footprint. It stands to reason that many members of the operations community would argue that classification as a weapon system has not necessarily helped the AOC.

In Air Combat Command's opinion, though, in spite of the serious challenges faced during the transition, the AOC is better off today than it was 15 years ago, especially in terms of training its crews. A dedicated formal training unit at Hurlburt Field, Florida, established a program of record, provided a rigorous configuration and change-management process, and ultimately resulted in recognition by the operations community that the AOC is the crown jewel in the joint force air component commander's tactical air control system C2 concept. Additionally, assignment to an AOC tour is no longer considered a career-ending event for rated officers—quite a change from the perception in the 1990s when an assignment to a numbered air force staff or an AOC was widely seen as the kiss of death for promotion in the rated career fields.

AFSPC would not let the initial pains of the AOC experience deter us from pushing the cyberspace weapon system concept forward. Every program (fighters, bombers, and ISR) confronted its fair share of challenges, but without a program—something with a name attached to it—cyberspace systems would always fight for scraps in money and manpower. As we integrate these cyberspace weapon systems into the Air Force construct, perhaps we can learn from the challenges of es-

tablishing the AOC weapon system and avoid the same pitfalls and mistakes.

Final Thoughts

Through the cyberspace domain, the United States exploits other war-fighting domains. Practically all warfare these days relies on cyberspace—everything from communications, precision navigation and timing, attack warning, ISR, and C2. Designating cyberspace weapon systems will help the Air Force guarantee persistent cyberspace access and mission assurance for other critical weapon systems and domains that rely on cyberspace. By doing so, the service has made a commitment that cyberspace will receive the programmatic and budgetary attention necessary to sustain cyberspace operations, support the cyber mission teams, and drive towards the JIE. Furthermore, cyberspace operations supported by core weapon systems offer increased security, performance, flexibility, and overall capability unmatched in a less normalized environment. The operationalization of cyberspace is more than just a way for AFSPC to properly organize, train, and equip the cyberspace domain—it is the logical evolution of cyberspace to a true war-fighting domain and a critical enabler of all other such domains. ✪

Notes

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 June 2013), 303, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

2. Joint Publication 3-13, *Information Operations*, 27 November 2012, II-9, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

3. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* ([Washington, DC: Mandiant, 2013]), 2, 3, 20, 59, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

4. Air Force Policy Directive 10-9, *Lead Command Designation and Responsibilities for Weapon Systems*, 8 March 2007, http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afpd10-9/afpd10-9.pdf.

Brig Gen Robert J. Skinner, USAF

General Skinner (BS, Park College; MS, Oklahoma City University) is the deputy commander, Air Forces Cyber (AFCYBER). He is the primary liaison and personal representative to US Cyber Command and the National Security Agency; he also supports AFCYBER's operational activities with the Office of the Secretary of Defense, Director of National Intelligence, Central Intelligence Agency, and other National Capitol Region cyber stakeholders. Commissioned in 1989, the general is a graduate of Squadron Officer School, Command and General Staff College, Air War College, and the Industrial College of the Armed Forces. His career highlights include wing and group commands, multiple squadron commands, a variety of tactical and fixed communications assignments as well as staff assignments at the Joint Staff, Air Staff, and a numbered air force. Prior to assuming his current position, General Skinner served as inspector general at Headquarters Air Force Space Command, Peterson AFB, Colorado. In this role, he led a 70-person, three-division directorate consisting of five branches charged with evaluating the readiness of more than 300 Air Force Space Command space and cyber units located at over 100 worldwide locations.

Let us know what you think! Leave a comment!