ANNEX 3-12 CYBERSPACE OPERATIONS

CATALOG OF DOCTRINE TOPICS

Introduction to Cyberspace Operations
The Operational Environment
US National Cyberspace Policy
Challenges of Cyberspace Operations
Threats to Cyberspace Operations
The Airman's Perspective
Integration of Cyberspace Operations Across Domains
Policy Related To Command and Organization Of Cyberspace Forces
Organization of Cyberspace Forces
Command and Control Of Cyberspace Forces
Authorities and Legal / Law Enforcement Considerations and Constraints
Design of Cyberspace Operations
Planning Cyberspace Operations
Execution of Cyberspace Operations
Assessment of Cyberspace Operations
Authorities and Legal Considerations
Considerations Across The Range of Military Operations
Appendix A: CSAF Remarks On Cyberspace
Appendix B: Policy And Doctrine Related To Cyberspace Operations

INTRODUCTION TO CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

Cyberspace superiority may be localized in time and space, or it may be broad and enduring. The concept of cyberspace superiority hinges on the idea of preventing prohibitive interference to joint forces from opposing forces, which would prevent joint forces from creating their desired effects. "Supremacy" prevents effective interference, which does not mean that no interference exists, but that any attempted interference can be countered or should be so negligible as to have little or no effect on operations. While "supremacy" is most desirable, it may not be operationally feasible. Cyberspace superiority, even local or mission-specific cyberspace superiority, may provide sufficient freedom of action to create desired effects. Therefore, commanders should determine the minimum level of control required to accomplish their mission and assign the appropriate level of effort.

Cyberspace. Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1]

Cyberspace operations. **"**The employment of cyberspace capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[2]

Cyberspace superiority. The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference.[3]

[1] Joint Publication (JP) 3-12(R [redacted]), *Cyberspace Operations*
[2] JP 3-0, *Joint Operations*
[3] Approved Air Force Space Command (AFSPC) definition of cyberspace superiority, derived from multiple AFSPC and LeMay Center cyberspace operations working groups, 2009-2010.

UNDERSTANDING CYBERSPACE

Cyberspace is a domain. Cyberspace operations are not synonymous with information operations (IO). IO is a set of operations that can be performed in cyberspace and other domains. Operations in cyberspace can directly support IO and non-cyber based IO can affect cyberspace operations.

Cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land, maritime, and space. It requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can create effects in and through cyberspace.

Even though networks in cyberspace are interdependent, parts of these networks are isolated. Isolation in cyberspace exists via protocols, firewalls, encryption, and physical separation from other networks. For instance, classified networks such as the US Armed Forces Secure Internet Protocol Router network (SIPRnet) are not hardwired to the Internet at all times, but connect to it via secure portals. Additionally, the construction of some hard-wired networks isolates them from most forms of radio frequency (RF) interference. These factors enable these networks to be isolated within cyberspace, yet still allow controlled connectivity to global networks.

Cyberspace segments are connected and supported by physical infrastructure, electronic systems, and portions of the electromagnetic spectrum (EMS).[4] As new systems and infrastructures are developed, they may use increasing portions of the EMS, have higher data processing capacity and speed, and leverage greater bandwidth. Systems may also be designed to change frequencies (the places where they operate within the EMS) as they manipulate data. Thus, physical maneuver space exists in cyberspace.[5]

Logical maneuverability in cyberspace is often a function of the security protocols used by host systems. Systems seeking connectivity with a secure host will have more difficulty gaining access than systems seeking connectivity with unsecured hosts. Additionally, defense against entry by undesired systems resides in the code or logic of the host system. Once a connection between systems is established, a potential intruder must exploit a fault in logic to enter the system. Code writing can thus be a form of logical maneuver in cyberspace. The potential intruder writes malicious code to

[4] Definition of EMS: "The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands." (JP 3-13.1)

[5] For additional information on the "Physical, Syntactic, and Semantic layers of Cyberspace" see Chapter 10 of "*Conquest in Cyberspace,"* Libicki, Martin C., RAND Corporation, Cambridge University Press, 2007.

gain maneuverability against targeted systems. As a defender becomes aware of unwanted presence within the system, the defender will alter the system's code to deny entry. The intruder, wishing to remain "on target," adapts the malicious code accordingly. This process is the equivalent of forces maneuvering to gain positions of advantage in the traditional air, land, space, and maritime domains. Both logical and physical maneuver space is required — one is often useless without the other.

ANNEX 3-12 CYBERSPACE OPERATIONS

THE OPERATIONAL ENVIRONMENT

Last Updated: 30 November 2011

The cyberspace domain is now a primary conduit for transactions vital to every facet of modern life. Our society and military are increasingly dependent on cyberspace. Cyberspace is a source of both strength and vulnerability for modern society. While cyberspace operations enable a modern society, they also create critical vulnerabilities for our adversaries to attack or exploit. Manufacturing controls, public utilities distribution, banking, communications, and the distribution of information for national security have shifted to networked systems. While this 30-year evolution has significantly benefited society, it has also created serious vulnerabilities. Increased wireless dependence and expanded interconnectivity has exposed previously isolated critical infrastructures vital to national security, public health, and economic well-being. Adversaries may attempt to deny, degrade, manipulate, disrupt, or destroy critical infrastructures through cyberspace attack, thus affecting warfighting systems and the nation as a whole. Recent incursions into Department of Defense (DOD) and Air Force networks underscore today's cyberspace challenge.

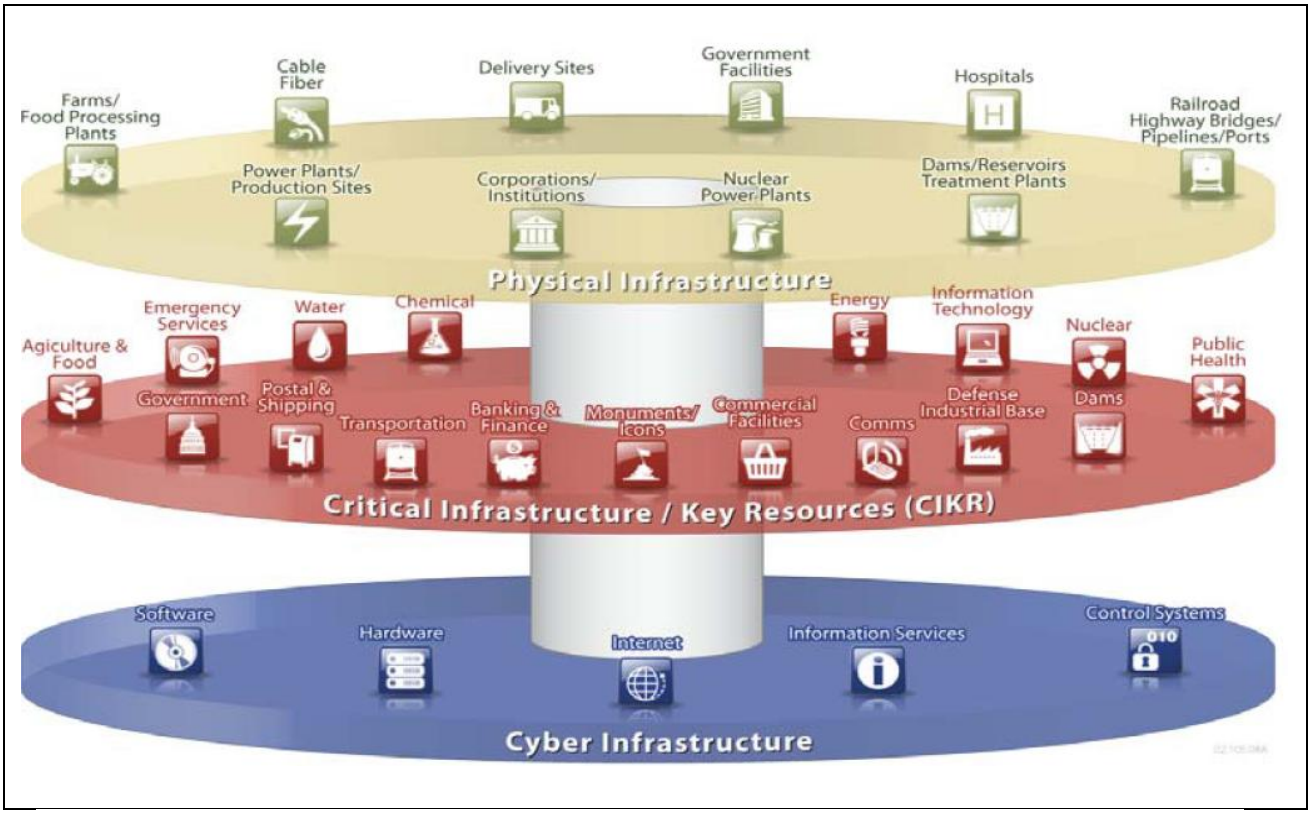
Adversaries in cyberspace are exploiting low-entry costs, widely available resources, and minimal required technological investment to inflict serious harm, resulting in an increasingly complex and distributed environment. The expanded availability of commercial off-the-shelf (COTS) technology provides adversaries with increasingly flexible and affordable technology to adapt to military purposes. Low barriers to entry significantly decrease the traditional capability gap between the US and our adversaries. Adversaries are fielding sophisticated cyberspace systems and experimenting with advanced warfighting concepts.

Cyberspace Infrastructure Relationships[1]

The Air Force depends upon the US' critical infrastructure and key resources for many of its activities, including force deployment, training, transportation, and normal operations. Physical protection of these is no longer sufficient as most critical

[1] Adapted from Dept. of Homeland Security: "Securing the Nation's Critical Cyber Infrastructure."

infrastructure is under the control of networked and interdependent supervisory control and data acquisition (SCADA) or distributed control systems (DCS).



Cyber Infrastructure

Since private industry is the primary catalyst for technological advancements, the military may become increasingly reliant on COTS technology. This reliance may present three primary vulnerabilities:

- Foreign ownership, control, and influence of vendors. Many of the COTS technologies (hardware and software) the Air Force purchases are developed, manufactured, or have components manufactured by foreign countries. These manufacturers, vendors, service providers, and developers can be influenced by adversaries to provide altered products that have built-in vulnerabilities, such as modified chips.

- Supply chain. The global supply chain has vulnerabilities that can potentially lead to the interception and alteration of products. These vulnerabilities are present throughout the product life cycle, from the inception of the design concept, to product delivery, and to product updates and support.

- COTS and government off-the-shelf (GOTS) balance. The vast majority of the Air Force's cyberspace operations components and capabilities are from COTS and to a much smaller degree, GOTS technologies.

ANNEX 3-12 CYBERSPACE OPERATIONS

US NATIONAL CYBERSPACE POLICY

Last Updated: 30 November 2011

There are many policy documents pertaining to cyberspace operations policy.

The documents most relevant to Air Force cyberspace operations are in Appendix B, Policy and Doctrine Related to Cyberspace Operations.

The National Strategy to Secure Cyberspace is the comprehensive strategy for the US to secure cyberspace. It spells out three strategic priorities:

- ✪ Prevent cyber attacks against America's critical infrastructure
- ✪ Reduce national vulnerability to cyber attacks
- ✪ Minimize damage and recovery time from cyber attacks

The *National Strategy to Secure Cyberspace* outlines the framework for organizing and prioritizing US Government efforts in cyberspace. This strategy guides federal government departments and agencies that secure cyberspace. It identifies the steps every individual can take to improve our collective cyberspace security.

The *National Military Strategy for Cyberspace Operations* (NMS-CO) is the comprehensive strategy for US Armed Forces to ensure US superiority in cyberspace. There are four strategic priorities of the NMS-CO:

- ✪ Gain and maintain initiative to operate within adversary decision cycles
- ✪ Integrate cyberspace capabilities across the range of military operations (ROMO)
- ✪ Build capacity for cyberspace operations
- ✪ Manage risk for operations in cyberspace

The NMS-CO describes the cyberspace domain, articulates cyberspace threats and vulnerabilities, and provides a strategic framework for action. The NMS-CO is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. The integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental to this approach.

CHALLENGES OF CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

Cyberspace operations offer unique military challenges. The paragraphs below address some of the known challenges: mission assurance, a compressed decision cycle, anonymity and the attribution challenge, and various threats inherent to cyberspace itself.

There is a requirement to balance defensive cyberspace actions within cyberspace with their impact on ongoing air, space, and cyberspace operations. The lack of situational awareness among domains can cause serious disconnects in one, significantly hindering operations in others.[1]

Mission Assurance

Mission assurance consists of measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions (MEFs), mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities.[2]

Mission assurance ensures the availability of a secured network to support military operations by assuring and defending the portion of the network directly supporting the operation. Cyberspace mission assurance begins by mapping the operation to the supporting architecture. Then, deliberate actions are taken to assure the availability of that portion of the network. These may include adding backups to single points of failure in the network or delaying certain maintenance actions to ensure the network will meet mission requirements. Second, the proactive actions are taken to ensure the network is secure and defended. These actions may include focusing the attention of network defense assets on the slice of the network supporting the operations and conducting operations to ensure no threats are resident on the network.

A “contested cyber environment” involves circumstances in which one or more adversaries attempt to change the outcome of a mission by denying, degrading, disrupting, or destroying our cyber capabilities, or by altering the usage, product, or our

[1] Office of Air Force Lessons Learned, *Enduring Airpower Lessons from OEF/OIF, Cyberspace Freedom of Action,* 20-25 April 2009, HQ USAF A9.
[2] United States Scientific Advisory Board, *Report on Defending and Operating in a Contested Cyber Domain,* SAB-TR-08-01, August 2008, p. 11.

confidence in those capabilities.[3]

Warfighters should realize risks and vulnerabilities are often created by the interdependencies inherent in the networking and integration of systems through cyberspace. Integration of cyberspace operations involves actions taken to enable decision superiority through command and control (C2), innovation, integration, and standardization of systems across air, space, and cyberspace domains. Integration means are tested via operational experiments like the Joint Expeditionary Force Experiment. Identifying vulnerabilities is difficult within a contested cyber environment. Our systems are open to assault and are difficult to defend. Some known examples of vulnerabilities in cyberspace operations are listed in the *National Military Strategy for Cyberspace Operations* (NMS-CO).

Assuring missions via cyberspace operations involves risk. Since the nature of cyberspace is interconnectivity, all cyberspace operations have inherent risk requiring constant attention and mitigation. Cyberspace is a domain with its own set of risks**.** In this domain, a risk assumed by one is potentially assumed by all**.** Mitigation of risk can result in a decreased risk level considered acceptable to continue conducting operations.[4] Examples of this kind of approach toward handling risk can be seen in many aspects. The implementation of firewalls, training, education, and intrusion detection and prevention systems represent types of risk mitigation.

Just as in the air domain, we do not defend the entire Cyberspace domain; we defend what is relevant to our operations. In cyberspace, this means protecting pathways and components, since action against critical systems could seriously degrade our ability to fight and win. Whether used offensively or defensively, however, conducting particular cyberspace operations may require access to only a very small “slice” of the domain. This does not mean “localized” in the sense of a limited geographical area (although that too may sometimes be required), but perhaps just a string of internet protocol (IP) addresses, which may span the globe but represent only a miniscule portion of data flow bandwidth. Similarly, it may involve the ability to hack through one particular firewall that may physically reside upon several servers, but which is never engaged physically only through virtual means. Finally, many operations may span only seconds from inception to conclusion, given the speed at which the Internet operates. Successfully operating in cyberspace may require abandoning common assumptions concerning time and space.

Freedom of action in cyberspace is a basic requirement for mission assurance. However, having the cyberspace capacity to achieve this freedom of action should not be taken for granted. Just as operating in the air domain requires having the capacity to

[3] Ibid.
[4] The White House, *National Military Strategy for Cyberspace Operations*, 2006.

do so (airborne platforms, runways, etc.), the Air Force should ensure it acquires sufficient capacity (bandwidth, components, etc.) to operate within cyberspace. Since access to cyberspace permeates daily activities, it is easy to overlook this requirement and assume that sufficient capacity will simply exist.

Cyberspace operations seek to ensure freedom of action across all domains for US forces and allies, and deny that same freedom to adversaries. Specifically, cyberspace operations overcome the limitations of distance, time, and physical barriers present in other domains. Exploiting improved technologies makes it possible to enhance the Air Force's global operations by delivering larger information payloads and increasingly sophisticated effects. Cyberspace links operations in other domains thus facilitating interdependent defensive, exploitative, and offensive operations to achieve situational advantage.

Potential adversaries wish to undermine mission assurance actions via cyberspace operations. The Air Force ensures it can establish and maintain cyberspace superiority and fight through cyberspace attacks at any time regardless if the US requires the use of military forces. Our adversaries have also demonstrated that they can create civil instability through cyber attacks. The Air Force maintains a capability to provide defense support to civil authorities in cyberspace when called upon by national leadership. Potential adversaries have declared and demonstrated their intent; Russia's relatively crude ground offensive into Georgia in 2008 was preceded by a widespread and well-coordinated cyberspace attack. The massive cyberspace attack and ensuing effects suffered by Estonia in 2007 illustrate how quickly malicious hackers affect even a technologically sophisticated government.

One last point to highlight concerning mission assurance is homeland infrastructure protection from threats or natural disaster. The Air Force should prepare to respond rapidly to mitigate effects of such threats or events and reconstitute lost critical infrastructure capabilities while also providing support to civil authorities as directed by competent authority. The Air Force should establish policies and guidance to ensure the execution of mission essential functions for critical infrastructure protection, in the event that an emergency threatens or incapacitates operations.

Compressed Decision Cycle of Cyberspace Operations

The fact that operations can take place nearly instantaneously requires the formulation of appropriate responses to potential cyberspace attacks within legal and policy constraints. The compressed decision cycle may require predetermined rules for intelligence, surveillance, and reconnaissance (ISR) actions.

Anonymity and the Inherent Attribution Challenge

Perhaps the most challenging aspect of attribution of actions in cyberspace is connecting a cyberspace actor or action to an actual, real-world agent (be it individual or state actor) with sufficient confidence and verifiability to inform decision- and policy-makers. Often this involves significant analysis and collaboration with other, non-cyberspace agencies or organizations. While cyberspace attribution (e.g., identifying a particular IP address) may be enough for some actions, such as establishing access lists (e.g., "white" or "black" lists of allowed or blocked IP addresses), attribution equating to positive identification of the IP address holder may be required for others, such as offensive actions targeting identified IP addresses.

The nature of cyberspace, government policies, and international laws and treaties make it very difficult to determine the origin of a cyberspace attack. The ability to hide the source of an attack makes it difficult to connect an attack with an attacker within the cyberspace domain. The design of the Internet lends itself to anonymity.

Anonymity is maintained both by the massive volume of information flowing through the networks, and by features that allow users to cloak their identity and activities. Nations can do little to combat the anonymity their adversaries exploit in cyberspace; however, the same features used by terrorists, hackers, and criminals, strengthen state surveillance and law enforcement capability, in modified form. Actions of anonymous or unidentified actors are akin to an arms race. Illicit actors continually amaze those in global law enforcement with the speed at which they stay one step ahead in the technology race. Nevertheless, nations have the advantage of law and the ability to modify the technological environment by regulation.

Anonymity is a feature of the Internet because of the way information moves through it and the way it is governed. The underlying architecture was intended to be robust, distributed, and survivable. The anonymous nature of the Internet is literally written into the structure of the Internet itself and cannot be dislodged without physically destroying many networks. The Internet was also designed where the intelligence was placed at the ends of the network, not in the network itself. Routing tools, software applications, and information requests come from the ends, in contrast to a traditional telephone network in which the switches, routing protocols, etc., are in the network itself. The difference makes it much harder to trace individual bits of information once they are in the network. The Internet's governance structure reflects its design.[5] This makes attribution a challenge.

---

[5] Ibid.

ANNEX 3-12 CYBERSPACE OPERATIONS

THREATS TO CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

In other domains, the primary threats to national security come from either nation states or transnational actors, such as terrorist organizations. Massive capital resources and personnel are required to build, field, maintain, and operate fighter aircraft, satellites, and ships, but it took only a small and determined organization with simple tools to fly into the World Trade Center buildings on September 11, 2001. Adversaries seek asymmetric advantages and cyberspace provides significant opportunities for obtaining them.

There are a variety of threats to cyberspace operations. The following paragraphs provide a brief description of each category of threat. These threats and others should be considered when conducting cyberspace operations.[1]

Nation State Threat. This threat is potentially the most dangerous because of access to resources, personnel, and time that may not be available to other actors. Other nations may employ cyberspace to attack and conduct espionage against the US. Nation state threats involve traditional adversaries and sometimes, in the case of espionage, even traditional allies. Nation states may conduct operations directly or may outsource third parties to achieve their goals.

Transnational Actor Threat. Transnational actors are formal and informal organizations that are not bound by national borders. These actors use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, destabilize confidence in governments, and conduct direct terrorist action.

Criminal Organization Threat. Criminal organizations may be national or transnational in nature depending on how they are organized. Criminal organizations steal information for their own use or, in turn, sell it to raise capital.

Individual or Small Group Threat. Individuals or small groups of people can illegally disrupt or gain access to a network or computer system—these people are better known as “hackers.” The intentions of hackers vary. Some are peaceful and hack into systems to discover vulnerabilities, sometimes sharing the information with the owners and some have malicious intent. Other hackers have political motivations and use

[1] See the *National Military Strategy for Cyberspace Operations*, (2006), for expanded descriptions.

cyberspace to spread their message to target audiences. Another type of hacker desires fame or status, and obtains it by breaking into secure systems or creating malware that creates havoc on commercial or government systems. Malware is the short name for "malicious software." Hackers can also be exploited by the other cyberspace threats, such as criminal organizations, in order to execute concealed operations against specific targets while preserving their identity or create plausible deniability.

In May 05, an unknown subject obtained unauthorized user level access to the Assignments Management System (AMS). Using this access, the subject was able to view information contained within the AMS, but was unable to alter information or gain access to any other Air Force computer systems. Computer records indicate that the subject gained access to AMS via a senior Air Force official's account. The compromised AMS account was set with privileges which allow the user to review any active duty Air Force members' single unit retrieval format (SURF) data from anywhere in the world with an Internet connection. SURF records contain sensitive data, such as assignment history, security clearance, personal identification information, rank, position, and duty status. The subject gained access to the web based account using the "forgot password" function to answer the challenge questions required to change the account password. The challenge questions asked for biographical information on the senior official, which was readily available on the Internet.

Upon review, it was determined that the senior USAF official's account had been used to view the SURF records of 37,069 Air Force members. Log analysis indicates the intrusion initially originated from forty-one different source IP addresses throughout the duration that the compromised account was used by the subject.

Throughout this duration the subject's activity originated from approximately twelve additional US based Internet Protocol (IP) addresses, which were later determined to be open proxies that the subject used to mask their true place of origin. There were no foreign based IP addresses used after the incident was reported. Court order subpoenas were served on all US-based source IP addresses from which the compromised AMS account was accessed; fifty in total. Information obtained via court order subpoenas identified the last known point of the origin. However, local law enforcement indicated that the information required to further identify the subject was no longer available.

—Air Force Office of Special Investigations Brief, June 2005

Traditional Threat. Traditional threats typically arise from states employing recognized military capabilities and forces in well-understood forms of military conflict. Within cyberspace, these threats may be less understood due to the continuing evolution of technologies and methods. Traditional threats are generally focused against the cyberspace capabilities that enable our air, land, maritime, special operations, and space forces and are focused to deny the US military freedom of action and use of cyberspace.

Irregular Threat. Irregular threats can use cyberspace as an unconventional asymmetric means to counter traditional advantages. These threats could also manifest through an adversary's selective targeting of US cyberspace capabilities and infrastructure. For example, terrorists could use cyberspace to conduct operations against our financial and industrial sectors while simultaneously launching other physical attacks. Terrorists also use cyberspace to communicate anonymously, asynchronously, and without being tied to set physical locations. They attempt to shield themselves from US law enforcement, intelligence, and military operations through use of commercial security products and services readily available in cyberspace. Irregular threats from criminal elements and advocates of radical political agendas seek to use cyberspace for their own ends to challenge government, corporate, or societal interests.

Catastrophic Threat. Catastrophic threats involve the acquisition, possession, and use of weapons of mass destruction (WMD) or methods producing WMD-like effects. While WMD attacks are physical (kinetic) events, they may have profound effects within the cyberspace domain by degrading or destroying key cyber-based systems vital to infrastructure like supervisory control and data acquisition (SCADA) systems. Well-planned attacks on key nodes of the cyberspace infrastructure have the potential to produce network collapse and cascading effects that can severely affect critical infrastructures locally, nationally, or possibly even globally. For example, an electromagnetic pulse could cause widespread damage to segments of the cyberspace domain in which operations must occur.

Disruptive Threat. Disruptive threats are breakthrough technologies that may negate or reduce current US advantages in warfighting domains. Global research, investment, development, and industrial processes provide an environment conducive to the creation of technological advances. The DOD should be prepared for the increased possibility of adversary breakthroughs due to continuing diffusion of cyberspace technologies.

Natural Threat. Natural threats that can damage and disrupt cyberspace include events such as floods, hurricanes, solar flares, lightning, and tornados. These types of events often produce highly destructive effects requiring the DOD to maintain or restore

key cyberspace systems. These events also provide adversaries the opportunity to capitalize on infrastructure degradation and diversion of attention and resources.

Accidental Threat. Accidental threats are unpredictable and can take many forms. From a backhoe cutting a fiber optic cable of a key cyberspace node, to inadvertent introduction of viruses, accidental threats unintentionally disrupt the operation of cyberspace. Although post-accident investigations show that the large majority of accidents can be prevented and measures put in place to reduce accidents, accidents should be anticipated.

Insider Threat. The “insider” is an individual currently or at one time authorized to access an organization’s information system, data, or network. Such authorization implies a degree of trust in the individual. The insider threat refers to harmful acts that trusted insiders might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual.

ANNEX 3-12 CYBERSPACE OPERATIONS

THE AIRMAN'S PERSPECTIVE

Last Updated: 30 November 2011

Airmen normally think of the application of force from a functional rather than geographical perspective. Airmen do not divide up the battlefield into operating areas as do surface forces; air mindedness entails thinking beyond two dimensions, into the dimensions of the vertical and the dimension of time.[1] Airmen leverage speed, range, flexibility, precision, time, and lethality to create effects from and within the air, space, and cyberspace domains.

Cyberspace operations are intrinsic to the conduct of modern military operations. "Airmen conduct a greater percentage of operations not just over the horizon but globally, expanding operations first through space and now also in cyberspace. Just as air operations grew from its initial use as an adjunct to surface operations, space and cyberspace have likewise grown from their original manifestations as supporting capabilities into warfighting arenas in their own right."[2] Thus, cyberspace operations should be tightly integrated with capabilities of the air and space domains into a cohesive whole, commanded by an Airman who takes a broader view of war, unconstrained by geographic boundaries.

[1] Volume 1, *Basic Doctrine*
[2] Ibid.

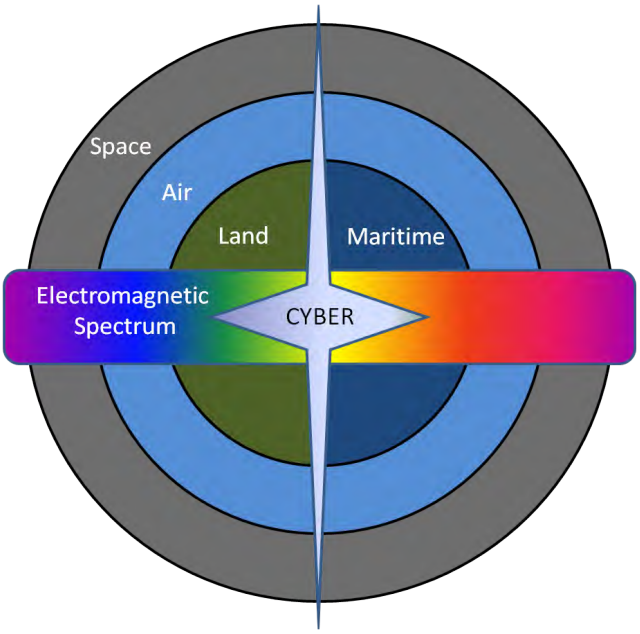
ANNEX 3-12 CYBERSPACE OPERATIONS

INTEGRATION OF CYBERSPACE OPERATIONS ACROSS DOMAINS

Last Updated: 30 November 2011

The core of cross-domain integration is the ability to leverage capabilities from different domains to create unique—and often "decisive"—effects. As the use of cyberspace continues to evolve, Airmen will determine new ways to solve problems to meet national objectives.

The figure on **Warfighting Operational Domain Relationships** portrays the relationship among the operational domains. This is important to consider because in modern warfare, all domains are interconnected via cyberspace operations.[1]



Warfighting Operational Domain Relationships

[1] Convertino, Sebastian, *Flying and Fighting in Cyberspace,* July 2007, Air University, p. 11.

ANNEX 3-12 CYBERSPACE OPERATIONS

POLICY RELATED TO COMMAND AND ORGANIZATION OF CYBERSPACE FORCES

Last Updated: 30 November 2011

According to the Deputy Secretary of Defense (DepSecDef), all combatant commands, military departments, and other defense components need the ability to operate unhindered in cyberspace; the domain does not fall within the purview of any one particular department or component. The Unified Command Plan assigns US Strategic Command (USSTRATCOM) the mission of synchronizing planning for cyberspace operations, in coordination with other combatant commanders (CCDRs), the Services, and, as directed, other US government agencies; and executing selected cyberspace operations. To support USSTRATCOM's cyberspace mission requirements, the commander of USSTRATCOM (CDRUSSTRATCOM) further delegated operational control (OPCON) or tactical control (TACON) of designated cyber forces to the commander of US Cyber Command (CDRUSCYBERCOM).[1]

[1] Derived from USCC CONOPS, dated 21 Sep 2010.

ANNEX 3-12 CYBERSPACE OPERATIONS

ORGANIZATION OF CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

The Air Force organizes, trains, and equips its cyber forces to support the combatant commanders (CCDRs) and the joint warfighters, and to accomplish Service functions. Joint cyberspace forces are an integral part of military operations, and command relationships are crucial for ensuring timely and effective employment. Commander, US Strategic Command (CDRUSSTRATCOM) advocates, plans, and executes military cyberspace operations and has the responsibility to prioritize, deconflict, integrate, and synchronize military cyberspace operations for current and planned joint operations. The Air Force presents some cyberspace forces to CDRUSSTRATCOM for day-to-day operations via its Service element, 24th Air Force (AFCYBER). US Northern Command (USNORTHCOM) and US Pacific Command (USPACOM) may conduct the civil support and homeland defense (HD) missions with cyberspace operations during critical infrastructure protection.[1] Like all Air Force forces, Air Force cyberspace forces may be assigned or attached to other CCDRs, coalition or joint force commanders, as directed.

United States Strategic Command (USSTRATCOM)

USSTRATCOM is responsible for synchronizing the planning of cyberspace operations.[2] The foundational command relationship for Air Force cyberspace forces under USSTRATCOM,[3] which:

- Directs global information grid (GIG) operations and defense.
- Plans against designated cyberspace threats.
- Coordinates with other combatant commands and appropriate US government agencies prior to the creation of cyberspace effects that cross areas of responsibility (AORs).
- Provides military representation to US national agencies, US commercial entities, and international agencies for matters related to cyberspace, as directed.

[1] See JP 3-27, *Homeland Defense,* 12 July 2007, p. 32.
[2] The phrase "synchronizing planning" pertains specifically to planning efforts only and does not, by itself, convey authority to execute operations or direct execution of operations.
[3] Derived from the 2008 Unified Command Plan.

- Advocates for cyberspace capabilities
- Integrates theater security cooperation activities, deployments, and capabilities that support cyberspace operations, in coordination with the geographic combatant commands (GCCs), and makes priority recommendations to the Secretary of Defense (SecDef).
- Conducts operational preparation of the environment (OPE) and intelligence preparation of the operational environment (IPOE) and, as directed, synchronizes execution with GCCs.
- Executes cyberspace operations, as directed.
- Plans, coordinates, and executes kinetic and non-kinetic global strike as required.

Each of these missions assigned by the Unified Command Plan (UCP) has key functions, roles and responsibilities the Air Force accomplishes in order to support Joint Functional Commands (JFCs).

United States Cyber Command (USCYBERCOM)[4]

Mission: USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified Department of Defense (DOD) information networks and prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/allied freedom of action in cyberspace and deny the same to our adversaries.

Focus: USCYBERCOM fuses the Department's full spectrum of cyberspace operations and plans, coordinates, integrates, synchronizes, and conducts activities to lead day-to-day defense and protection of DOD information networks, coordinate DOD operations providing support to military missions, direct the operations and defense of specified DOD information networks, and prepare to, and when directed, conduct full spectrum military cyberspace operations. The command is charged with pulling together existing cyberspace resources and synchronizing warfighting effects to defend the information security environment.

USCYBERCOM centralizes command of cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters the DOD's cyber expertise. USCYBERCOM's efforts support the Armed Services' ability to confidently conduct high-tempo, effective operations as well as protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks.

[4] Fact Sheets "USCYBERCOM"

Forces: USCYBERCOM is a sub-unified command subordinate to USSTRATCOM. Service elements include:

USAF:	24th Air Force (AFCYBER)
USA:	Army Forces Cyber Command
USN:	Fleet Cyber Command
USMC:	Marine Forces Cyber Command

Air Force Space Command (AFSPC)

AFSPC organizes, trains, and equips Air Force cyberspace forces to conduct sustained operations in, through, and from cyberspace and fully integrates with air and space operations. It serves as the lead major command (MAJCOM) for Air Force cyberspace procedures and concepts of operations. As the Air Force Service component commander to CDRUSSTRATCOM for Air Force cyberspace forces, the commander, AFSPC (AFSPC/CC) exercises administrative control (ADCON) over active component and specified elements of ADCON over activated reserve component Air Force cyber forces assigned or attached to USSTRATCOM. This includes those Air Force forces assigned or attached as part of USCYBERCOM under 24th Air Force (24 AF). Operational control (OPCON) over assigned and attached Air Force cyberspace forces will be as directed by CDRUSSTRATCOM, normally through CDRUSCYBERCOM to the commander, 24 AF (24 AF/CC). AFSPC supports all joint warfighters in the cyberspace domain by providing forces, through 24 AF, that establish, maintain, operate, and defend Air Force cyberspace components; exploit adversary vulnerabilities; attack adversary systems; and provide command and control for assigned and attached cyberspace forces.[5]

See Volume 1, *Basic Doctrine* for additional doctrinal guidance on ADCON and specified ADCON responsibilities.

24th Air Force

This numbered Air Force serves as the component numbered Air Force (C-NAF) to USCYBERCOM. In this role, the C-NAF commander serves as the senior Air Force warfighter for employment of assigned and attached forces under USCYBERCOM. As commander of Air Force forces (COMAFFOR), the 24 AF/CC is normally delegated OPCON of assigned and attached Air Force forces and exercises control via the 624th Operations Center (624 OC).

The 24 AF/CC is further responsible for executing Air Force Service tasks as directed

[5] AFSPC Cyberspace PAD, Change 4.

by the Secretary of the Air Force (SECAF) and Chief of Staff of the Air Force (CSAF) in the role as the commander, Air Force Network Operations (AFNETOPS/CC). These tasks include overseeing the morale, welfare, safety, and security of assigned and attached forces. They also include tasks inherent in the responsibility to provide, establish, and maintain a secure and defensible network in accordance with Air Force Guidance Memorandum 13-01. Per this document, the AFNETOPS/CC is "the single commander responsible for the overall operation, defense, maintenance and control of the AF-GIG."

Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA)

Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) is a field operating agency subordinate to the Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (AF/A2). AFISRA organizes, trains, equips, presents, and integrates all-source intelligence (e.g., signals intelligence [SIGINT], geospatial intelligence [GEOINT], measurement and signature intelligence, human intelligence, etc.) and full-spectrum capabilities to the intelligence community and to JFCs through the COMAFFOR. It provides customers at all echelons with multi-source intelligence products, applications, and services and provides intelligence expertise in the areas of SIGINT, IO (including information protection), acquisition, foreign weapons systems and technology, and treaty monitoring. In relation to cyberspace, AFISRA serves as the Air Force Service cryptologic component to the National Security Agency/Central Security Service (NSA/CSS), which authorizes SIGINT operations under Title 50, United States Code (U.S.C.). While NSA-derived analytic work roles are essential to cyber operations, employing full-spectrum cyber effects requires a multi-INT analysis approach. To enable 24 AF (AFCYBER) operations, AFISRA provides all-source cyber-focused ISR including digital network analysis to 24 AF through the 659th ISR Group. This support is generally characterized within five cyber-focused ISR areas: current intelligence and reporting, indications and warning, threat attribution and characterization, IPOE, and computer network exploitation.

ANNEX 3-12 CYBERSPACE OPERATIONS

COMMAND AND CONTROL OF CYBERSPACE FORCES

Last Updated: 30 November 2011

See JP 1, *Doctrine for the Armed Forces of the United States*, and Volume 1 for additional doctrinal guidance on command relationships.

Command and Control (C2) Options. When contemplating C2 options for joint cyberspace operations within the operational area, the Joint Force Commander (JFC) can choose to exercise C2 through the joint force staff, through a Service component commander, or through a functional component commander by designating one of the Service component commanders. Many factors will weigh on the JFC's selection, most notably the type and availability of forces/capabilities to accomplish the assigned mission. Additional factors may include host and friendly nation support, level and commitment of coalition forces, enemy capabilities and actions, and environmental limitations.

Theater-Level Considerations. When the geographic combatant command (GCC) establishes a subordinate joint command to conduct operations, forces are normally attached as needed, with delegation of operational control (OPCON) to the subordinate JFC. However, the GCC also will weigh the operational circumstances and decide if available cyberspace forces/capabilities can be most effectively employed by the subordinate JFC(s), by retaining them at the GCC level, or a combination thereof. This decision requires careful consideration after a thorough dialogue among the joint and Service component/force commanders.

Global Cyberspace Operations

Air Force cyberspace capabilities are used around the globe daily. The Unified Command Plan (UCP) establishes US Strategic Command (USSTRATCOM) as the functional unified command with overall responsibility synchronizing planning for military cyberspace operations. CDRUSSTRATCOM exercises combatant command (command authority) (COCOM) of cyberspace forces assigned by the SecDef in the *Forces For Unified Commands* memorandum. CDRUSSTRATCOM has delegated OPCON to commander, US Cyber Command (CDRUSCYBERCOM) to employ these forces to support worldwide operations.

Some cyberspace capabilities require deconfliction with organizations outside assigned

areas of responsibility (AORs) due to collaboration with US government and partner nation organizations. Thus, theater and global cyberspace operations require a C2 system capable of collaborative design, planning, execution, and assessment across all affected AORs and with USSTRATCOM.

Cyberspace operations can be controlled as a global system operating as a single entity (for example, the Air Force portion of non-secure Internet Protocol Router Network), or by GCC's as part of theater operations. Global and theater cyberspace operations require different command relationships and levels of coordination to create desired effects.

Theater Cyberspace Integration

Cyberspace effects are created through the integration of cyberspace capabilities with air and space capabilities. The boundaries within which cyberspace C2 is exercised and the priorities and restrictions on its use should be identified in coordination with the JFC, non-DOD governmental agencies, and national leadership. The potential for cyberspace effects to cause strategically important consequences may often necessitate coordination with the highest levels of US and partner nation governments.

Theater commanders integrate cyberspace effects throughout joint and coalition military operations. Certain cyberspace forces move forward to conduct operations in specific theaters. Some organic cyberspace forces may also be assigned to particular theaters.

Even in the case of global functional C2, cyberspace experts normally are assigned to theater staffs to facilitate cyberspace integration. USSTRATCOM should provide representation to theater JFCs. For the Air Force, cyberspace expertise resides in each AOC. When requested to serve on theater staffs, the 24 AF presents expertise via an AF cyber liaison element to assist coordinating, deconflicting, synchronizing, and integrating global and theater cyberspace operations.

Air Force Presentation of Cyberspace Forces

Regional Organization and Control. In response to a military situation, a combatant commander (CCDR) will normally organize a joint task force (JTF). If the entire theater is engaged, the CCDR may be the JFC. If the contingency is less than theater-wide, the CCDR may establish a subordinate JTF commanded by a subordinate JFC. In either case, the CCDR will first look to assigned in-theater forces. If augmentation is required, the JFC will request additional forces through the SecDef. Upon SecDef approval, additional forces will transfer into the theater and will be attached to the gaining CCDR, and the degree of control gained over those forces (i.e., OPCON or tactical control [TACON]) will be specified in the deployment orders. The gaining CCDR then normally delegates OPCON of these forces downward to the JTF commander who

should, normally, delegate OPCON to the Service component commanders within the gaining JTF. All Air Force forces assigned or attached to a joint task force, or established as a single-Service task force, should be organized and presented as an air expeditionary task force (AETF).

- Within a joint force, the JFC may organize forces in a mix of Service and functional components. All joint forces contain Service components, because administrative and logistical support for joint forces are provided through Service components. Therefore, by definition, every joint force containing assigned or attached Air Force forces will have a commander of Air Force forces (COMAFFOR).

- The COMAFFOR normally exercises OPCON over Air Force forces within the AETF.

Functional Organization and Control. Not all air, space, and cyberspace forces employed in an operation will be attached forward to a geographic CCDR. Some Air Force forces are capable of serving more than one CCDR at a time. Such forces, such as inter-theater air mobility, space, and special operations forces, are organized under functional CCDRs to facilitate optimal use of cross-AOR forces. When such forces are deployed in a GCC's AOR, they will often remain under the OPCON of their respective functional CCDR and operate in support of the geographic CCDR. The SecDef establishes support relationships between the CCDRs for the planning and execution of joint operations.[1]

Normally, a support relationship is formally established between a GCC and USSTRATCOM. In some circumstances, after coordination with the owning commander and upon SecDef approval, control of functional forces may be transferred to a geographic commander with specification of OPCON or TACON.

OPCON over assigned and attached Air Force cyberspace forces will be as directed by CDRUSSTRATCOM, normally through CDRUSCYBERCOM to the 24 AF/CC. As the COMAFFOR, the 24 AF/CC normally exercises OPCON of assigned and attached Air Force forces through the 624th Operations Center (624 OC).

For more detailed information concerning presentation of forces, see Volume 1, Basic Doctrine.

The JFC may elect to establish functional component commands to integrate specific capabilities across the joint force. The JFC normally appoints a joint force air component commander (JFACC) who is responsible for air effects within the theater. When the theater COMAFFOR is designated the JFACC, the COMAFFOR is prepared to command joint cyberspace forces as well as joint air forces since the JFC may also

[1] JP 1, *Doctrine for the Armed Forces of the United States.*

delegate authority for cyberspace effects to the JFACC. The JFC specifies the elements of TACON to be exercised over forces made available. Some cyberspace forces may be attached to a COMAFFOR/JFACC even though they may remain at home station.

AUTHORITIES AND LEGAL / LAW ENFORCEMENT CONSIDERATIONS AND CONSTRAINTS

Last Updated: 30 November 2011

Command, control, and organization of Air Force cyberspace forces are designed with inherent flexibility and versatility. These characteristics ensure Air Force cyberspace mission accomplishment across the range of military operations (ROMO).

Legal considerations and international legal obligations apply to the employment of cyberspace capabilities. International law, domestic law and policy decisions, the law of armed conflict, and rules of engagement establish the legal framework within which operational activities are evaluated.

In certain situations, law enforcement authorities may be the driving forces for certain actions in military cyberspace operations. In these situations, law enforcement organizations (e.g., the Air Force Office of Special Investigation and Federal Bureau of Investigation) do three things: 1) make cases against criminals who represent a threat via cyberspace; 2) apprehend cyberspace criminals; and 3) preserve evidence of a cyberspace crime. The authority of cyberspace law enforcement agencies is driven by jurisdiction.

Mutually beneficial national interests govern coalition cyberspace force involvement. Coalition forces are integrated as needed and are tailored to each situation or operation based on the national interests of both the US and partner nations. The level of coalition integration is directly influenced by the partnerships or agreements made with the partner nation involved.

Across the ROMO, cyberspace forces may at one moment be operating under authorities flowing from provisions of Title 10, U.S.C., *Armed Forces*, and another under Title 50, U.S.C., *War and National Defense*. In addition, Air National Guard (ANG) cyberspace forces may be training under Title 32, U.S.C., *National Guard*. Guardsmen in Title 32 status may train for Title 10 missions but may not execute them. The rules for operating under these different titles of US law are very different and the authority to transition from one to another may be held at a very high level, even that of the President, although the individual conducting the operation and his/her immediate supervisors may be tactical-level “operators.” It is important that individuals be clearly

aware of the authority for each operation they are a part of, and the legal parameters that implies.

The employment of forces within this varied legal landscape emphasizes the need for clearly delineated command relationships. This is particularly true when reserve component forces (reserve or ANG) are being utilized. The authority that may be exercised varies with duty status and command relationships. Particular care should be given to clearly delineating command relationships that apply during various states of reserve component employment and training.

ANNEX 3-12 CYBERSPACE OPERATIONS

DESIGN OF CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

Cyberspace operations may be conducted in a variety of situations and circumstances. The decision of which cyberspace capabilities to employ is based not only on overall joint campaign or operation objectives, but on the risks of possible adversary responses and other potential second and third order effects on the campaign or operation.

In cyberspace, the time between execution and effect can be milliseconds. Nonetheless, the observe-orient-decide-act (OODA) loop remains a valid construct for examining the decision cycle in cyberspace. Ongoing operations can be considered those operations that span past the phases of warfare.

Even for ongoing operations, planning at the strategic level is imperative because cyberspace operations can create effects simultaneously at the strategic, operational, and tactical levels across multiple domains. Planners should provide inputs to and receive feedback from appropriate intelligence and targeting organizations across the full range of government organizations and partner nations. Cyberspace's unique attributes and potential for speed require the ability to react to rapidly changing situations.

Inclusion of cyberspace superiority strategy in formal planning normally offers many planning and execution options to meet a theater JFC's objectives. Cyberspace operations can enable creation of many effects that formerly required physical attack to accomplish. Descriptions of these processes can be found in JP 5-0, *Joint Operation Planning*.

ANNEX 3-12 CYBERSPACE OPERATIONS

PLANNING CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

Airmen should be prepared to articulate to commanders the advantages that cyberspace operations can provide, as well as the dangers of unintended and undesirable effects and the need for close coordination between the many agencies with a role in cyberspace operations. Cyberspace operations normally are planned as part of major operations and campaigns, homeland operations, crisis response, and limited contingency operations. In these cases, planning is normally fully integrated into the joint operations planning process at the JFC level and in the joint operation planning process (JOPP) at the component level.

Security versus Capability

Planners should consider the impact of increasing security in cyberspace on operations. Changing information operations conditions or deploying additional tools to analyze networks can cause slower network operation speeds. In a bandwidth-limited environment or in an environment with many dispersed forces, planners should account for impacts of how measures designed to improve cyberspace defenses could actually hinder or desynchronize operations.

Logistics Support

Readiness and sustainability of cyberspace capabilities are directly related to the quality of logistics planning. Cyberspace logistics programs should be developed in balance with modernization efforts and the operating capability each category of resources provides. Emphasis should be on total effectiveness to maximize cyberspace operations capabilities.

ANNEX 3-12 CYBERSPACE OPERATIONS

EXECUTION OF CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

During the execution stage, cyberspace operators within the air operations center (AOC) will integrate cyberspace effects into the commander, Air Force forces (COMAFFOR)/joint force air component commander's (JFACC's) time-phased scheme of maneuver and fires based on commander's guidance, desired effects, friendly capabilities, and likely adversary courses of action. US Strategic Command (USSTRATCOM) cyberspace support may be obtained through the supported/supporting relationship and should be fully integrated into the COMAFFOR/JFACC's planning and execution.

Global Operations

The tasking cycle for cyberspace operations is the process the 624th Operations Center (624 OC) uses to translate commander US Cyber Command (CDRUSCYBERCOM) and theater JFC's objectives, priorities, and intent into a coherent, executable plan for Air Force cyberspace forces. The 624 OC's process is a derivative of the Joint Operations Planning Process–Air (JOPP-A). The Air Force cyber tasking order (CTO), a key product of the tasking cycle, is used to task and execute assigned and attached cyberspace forces. The cyber tasking order is analogous to an air tasking order. The cyber tasking cycle, which is based on the air tasking cycle, is an iterative process for planning, coordinating, apportioning, allocating, executing, and assessing the effectiveness of cyberspace operations. The cycle can be lengthened or shortened to synchronize with the theater battle rhythm to support crisis. It includes continuous collection, correlation, and prioritization of many inputs to meet CDRUSCYBERCOM and theater JFC's intent and objectives.

The CTO is derived from CDRUSCYBERCOM orders and, when supported, JFC's orders. It tasks assigned and attached cyberspace forces, provides guidance for synchronization of global and theater joint air, space, and cyberspace operations, and provides special instructions for the period it covers. Every cyberspace operation during that period should be on the CTO for situational awareness and deconfliction purposes.

Theater Operations

The air and space tasking cycles are the processes the theater AOC uses to translate JFC objectives, priorities, and intent into a coherent, executable plan for assigned and attached Air Force forces. The air operations directive and the air tasking order (ATO) are key products of the air and space tasking cycle.

The joint air and space operations plan reflects the COMAFFOR/JFACC's integrated air, space, and cyberspace operations plan to support the JFC's campaign. It should include the tasking of all assigned or attached cyberspace forces and all requests for theater support from global cyberspace forces. Air Force cyberspace forces that are assigned or attached with specification of operational control (OPCON) or tactical control (TACON) to a theater COMAFFOR/JFACC are integrated into operations via the air tasking cycle and tasked via the ATO.

Integration and Synchronization of Theater and Global Operations

When the 624 OC is supporting a theater operation, the CTO is synchronized with the theater ATO throughout the tasking cycle, with theater operators working closely with those at the 624 OC. If supporting a single, primary theater, the tasking cycle is synchronized with that theater's tasking cycle to optimize cyberspace support to the theater. The 624 OC, using guidance from the COMAFFOR/JFACC, helps develop cyberspace courses of action in support of theater operations. During the planning phase, the 624 OC uses COMAFFOR/JFACC guidance, rules of engagement (ROE), the joint integrated prioritized target list, the target nomination list, and the approved master air attack plan (MAAP), to finalize the CTO. After the ATO is finalized, the theater AOC forwards it to all required users to include the 624 OC. During execution, cyberspace tasking can occur dynamically to meet supported commander's requests.

ASSESSMENT OF CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

Assessment encompasses efforts, at all levels of conflict, use logical and defensible constructs to evaluate effects, gauge progress toward accomplishment of actions and objectives, and make strategy recommendations to shape future action. Assessments of operations conducted in and through cyberspace follow the same general procedures as the assessment of all other operations and are informed by a range of inputs, including intelligence, surveillance, and reconnaissance (ISR), munitions effectiveness, and operational reporting.

There are two primary types of assessments accomplished at the operational level, tactical and operational-level. Tactical assessment (TA) is generally performed by the air operations center's (AOC) ISR division and focuses on the effectiveness of tactical operations. Operational-level assessment (OA) of strategy is usually executed within the strategy division, provides insights and recommendations on the relevant commander's (i.e., commander, Air Force forces (COMAFFOR), joint force air component commander (JFACC) or commander, 24th Air Force (24 AF/CC)) strategy.

Tactical Assessment (TA)

TA is the overall determination of the effectiveness of tactical operations. It consists of the evaluation of tactical actions against assigned tactical tasks using empirical, objective, and usually quantifiable measures for collection and analysis. TA analysts collect, aggregate, analyze, and archive relevant data. This level of assessment determines commander need to take further tactical action. TA answers such questions as: "*Was the intended action accomplished?," "Was the intended direct effect created?," "Has the target's status changed?," and "Is re-engagement, re-attack, or 're-influence' necessary?"*

To make assessment most effective, measures and indicators should be determined during the planning process. TA of an operation is based on post-mission analysis. Task accomplishment and resulting potential direct effects are measured through a variety of intelligence and analytical methods, including signals intelligence (SIGINT) and geospatial intelligence (GEOINT), among other means.

Indirect effects, such as potential changes in behavior that are very difficult to assess in a time-sensitive manner, are best assessed at the operational level and above.

Operational-Level Assessment (OA)

OA is an analytically supported judgment of a commander's strategy (ends, ways and means). This type of assessment is the first level at which complex indirect effects are normally evaluated, progress toward operational and strategic objectives is measured, and recommendations for strategy adjustments and future action extending beyond re-attack are made.

Assessment at the operational level focuses on both effects and performance via measures of effectiveness (MOE) and measures of performance (MOP), respectively. MOEs are "used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect."[1] MOPs are "used to assess friendly actions that [are] tied to measuring task accomplishment."[2] In short, MOEs help measure progress toward the end state while MOPs are used to measure the strategy's ways and means. These measures should flow from the development of criteria that define the conditions required to receive specific assessment grades. This grading of the strategy's ends, ways, and means is often presented using a stoplight chart – with specific criteria designated for red, yellow, and green – in order to yield consistent, meaningful, and understandable feedback to the commander.

In order to accomplish this assessment process within the interrelated and complex nature of many cyberspace operations, operational-level cyberspace planners and analysts should develop an intimate understanding of the linkage between cyberspace and the supported mission or operation. This requires direct feedback from those closest to observing the intended effects, such as the Airmen executing cyber-enabled Air Force missions or the warfighters in theater, in order to assess the level of cyberspace performance and effectiveness. For example, the assessment of cyberspace operational effects in support of influence operations requires an in-depth understanding of the warfighter's desired impact on behavior and the ability to measure any resulting behavioral changes.

Situation Reporting

In addition to the assessment provided by the strategy team regarding conduct of combat operations, the COMAFFOR/JFACC and 24 AF/CC should receive daily reports on the status of friendly forces. Commanders should prioritize assets by their criticality

[1] JP 3-0
[2] Ibid.

to operations and have situational awareness of their linkages in the domain. In addition, they should anticipate cascading effects of degraded operations similar to attacks on assets in other domains. Additionally, the 24 AF/CC should ensure situation reporting is operationally-focused and addresses enemy actions and attacks, friendly actions taken to mitigate threats, and subsequent impact on friendly forces.

ANNEX 3-12 CYBERSPACE OPERATIONS

AUTHORITIES AND LEGAL CONSIDERATIONS

Last Updated: 30 November 2011

Authorities

Cyberspace forces will normally conduct operations under the authority of Title 10, U.S.C., *Armed Forces* or Title 50, U.S.C., *War and National Defense*. The authorities invoked will differ depending on the type of operation being conducted. The rules for operating under these varying titles are different. Authorities to act against adversaries are included in the execute order or operation order for a specific operation. If aggressive defensive responses or counter-offensive operations are authorized, authorities should be clearly defined and understood. Cyberspace forces belonging to the Air National Guard (ANG) are governed in peacetime by Title 32, U.S.C., *National Guard*.

Legal Considerations

Cyberspace operations may be conducted at any level of war and, within legal parameters, in support of global and theater objectives.

Legal considerations and international legal obligations apply to the employment of cyberspace capabilities. International law, domestic law and policy decisions, the law of armed conflict, and rules of engagement establish the legal framework within which operational activities are evaluated. Usually, the staff judge advocate on a commander's staff advises the given commander on the lawful means of conducting cyberspace operations as detailed in JP 1-04, *Legal Support to Military Operations*. Sound legal advice throughout the planning and execution of cyberspace operations is essential to mission success. This is especially important while courses of action are being developed and before they are executed. Early identification of legal issues will maximize planning efforts by developing lawful courses of action early in the planning process. The legal support staff should have access (billets and clearances) to the information, processes, and programs used in cyberspace operations and understanding of the underlying cyber technologies.

CONSIDERATIONS ACROSS THE RANGE OF MILITARY OPERATIONS

Last Updated: 30 November 2011

Engagement and Cooperation Operations

Multinational operations are becoming the norm for military operations, making intelligence and information sharing with allies and coalition partners increasingly important. Connectivity is essential, particularly when the US, allies, and coalition host nation forces function in mutual support during combat operations. Interoperability issues should also be considered in light of the Air Force's need for information assurance. As a part of a larger networked team, the Air Force should plan and execute in complete concert with other Services, nations, and agencies.

Homeland Operations

Cyberspace capabilities play a major role in homeland operations (e.g., disaster relief) when they are needed to rebuild portions of the cyberspace domain or to restore access to the domain. Timely and coordinated US government responses are important when establishing and reconstituting cyberspace capabilities.

Attack and exploitation operations in a homeland defense (HD) scenario may involve complex legal and policy issues; however, these issues do not prevent the application of attack and exploitation operations for HD, but temper it. Unless approved by appropriate authorities, Department of Defense (DOD) assets cannot be used to perform attack or exploit operations on US entities. Also, information sharing protocols, laws, and policies regulate, and at times may prevent, data and information sharing between agencies, organizations, and nations, thereby potentially reducing knowledge development. Protection of classified and sensitive information may also preclude effective sharing with other agencies and coalition partners

Establishing the Cyberspace Infrastructure in Afghanistan

In 2007, in support of Operation ENDURING FREEDOM, the 3rd Combat Communication Group (3 CCG) deployed to Kabul, Afghanistan and established an Enterprise Network for Afghanistan's Ministry of Interior (MoI) which provides capabilities such as e-mail, telephone service through "voice over Internet protocol" and video teleconferencing capability between the National Police Coordination Center, six joint regional coordination centers, 12 Kabul headquarters buildings, 38 provincial command centers as well as about 200 other locations such as medical and fire stations. Also, 3 CCG provided the infrastructure to allow network technicians to protect MoI's computers against viruses and provided a platform from which they can defend against cyber-attack.

Properly implemented cyberspace operations support defense of the homeland. When a domestic incident occurs, the escalation processes inherent in civil support procedures are implemented. A non-DOD civilian agency is in charge of civil support incidents, and military assistance is provided through a relationship similar to direct support, as articulated in civil support agreements and the Standing civil support execution order (EXORD). In all cases, the Air Force is prepared to support homeland operations through intelligence and information sharing within the appropriate legal

Reconstituting the Cyberspace Infrastructure during Disaster Relief

In 2005, the US's Gulf of Mexico region was devastated by a hurricane which destroyed critical infrastructure in Mississippi, Louisiana, and Texas. This disaster displaced tens of thousands of people seeking to escape the impact of the storm. Based on their expertise for extending the cyberspace domain, Air Force combat communications groups deployed throughout the Gulf region to reconstitute the cyberspace domain and allow military and US government organizations to communicate and be connected for situational awareness and C2.

framework.

Crisis Response and Limited Contingency Operation Considerations

These missions may be operations into friendly nations; however, some states are unstable and may include elements that are actively hostile toward the US. In other situations, political or international considerations may require air operations to be conducted within known threat areas. Cyberspace forces may or may not have to deploy to support these operations.

Major Operations and Campaigns

In addition to other ongoing missions, cyberspace operations can be planned as part of major operations and campaigns. In these cases, planning should be fully integrated into the joint operation planning process at the JFC level and the joint operations planning process for Air at the component level. Descriptions of these processes can be found in JP 5-0, *Joint Operation Planning*, and Annex 3-0, *Operations and Planning*. This kind of operational planning does not significantly differ from planning for operations in other domains in terms of processes, thus this section concentrates upon the continuous, cyclic, and iterative nature of ongoing cyberspace operations.

Inclusion of a strategy for cyberspace superiority in formal planning offers commanders many “non-traditional” options. Cyberspace operations enable creation of effects that formerly required physical attack to accomplish. Cyberspace operations also open avenues for exploitation of adversary capabilities and for changing the information that the adversary receives. This type of effect may not be possible through access in the other physical domains.

During the execution stage of major operations and campaigns, cyberspace planners and operators should work in conjunction with the commander of Air Force forces’ (COMAFFOR) time-phased scheme of maneuver for a given tasking period. Planners should synthesize commander’s guidance, desired effects, supported components’ schemes of maneuver, friendly capabilities, and likely adversary courses of action. Operators will employ friendly resources against approved targets.

APPENDIX A: CSAF REMARKS ON CYBERSPACE

Last Updated: 30 November 2011

1. The United States is vulnerable to cyberspace attacks by relentless adversaries attempting to infiltrate our networks at work and at home – millions of times a day, 24/7.

2. Our adversaries plant malicious code, worms, botnets, and hooks in common websites, software, and hardware such as thumbdrives, printers, etc.

3. Once implanted, this code begins to distort, destroy, and manipulate information, or "phone" it home. Certain code allows our adversaries to obtain higher levels of credentials to access highly sensitive information.

4. The adversary attacks your computers at work and at home knowing you communicate with the Air Force network by email or by transferring information from one system to another.

5. As cyber wingmen, you have a critical role in defending your networks, your information, your security, your teammates, and your country.

6. You significantly decrease our adversaries' access to our networks, critical Air Force information, and even your personal identity by taking simple action.

7. Do not open attachments or click on links unless the email is digitally signed, or you can directly verify the source—even if it appears to be from someone you know.

8. Do not connect any hardware or download any software, applications, music, or information onto our networks without approval.

9. Encrypt sensitive but unclassified and/or critical information. Ask your computer security administrator for more information.

10. Install the free Department of Defense anti-virus software on your home computer. Your computer security administrator can provide you with your free copy.

— **Gen Norton A. Schwartz, Chief of Staff, US Air Force**
"Defending Our Networks and Our Country"

APPENDIX B: POLICY AND DOCTRINE RELATED TO CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

National-Level Documents	
National Security Strategy	The National Security Strategy of the United States of America is a document prepared periodically by the executive branch of the government of the United States for congress that outlines the major national security concerns of the United States and how the administration plans to deal with them. The legal foundation for the document is spelled out in the Goldwater-Nichols Act. The document is purposely general in content (contrast with the National Military Strategy) and its implementation relies on elaborating guidance provided in supporting documents (including the National Military Strategy [NMS]).
US *National Strategy to Secure Cyberspace*, February 2003	Covers the necessity for vigilance in cyberspace, many defensive aspects of cyberspace operations, and the general principles that should guide national response to a cyberspace "crisis."[1]

Department of Defense Documents	
National Defense Strategy (NDS)	The NDS is issued periodically and the last one was published in June 2008. It outlines how the Department supports the President's National Security Strategy and informs the National Military Strategy and other subordinate strategy documents. The strategy builds on lessons learned and insights from previous operations and strategic reviews such as the 2006 Quadrennial Defense Review.

[1] *National Strategy for Securing Cyberspace*, The White House, February 2003.

Department of Defense Documents	
National Military Strategy	The NMS is issued by the Chairman of the Joint Chiefs of Staff as a deliverable to the Secretary of Defense briefly outlining the strategic aims of the armed Services. The NMS's chief source of guidance is the National Security Strategy document. The Chairman of the Joint Chiefs of Staff, in consultation with the other members of the Joint Chiefs of Staff, the Commanders of the Unified Combatant Commands, the Joint Staff, and the Office of the Secretary of Defense, prepares the National Military Strategy in accordance with 10 U.S.C., Section 153. Title 10 requires that not later than February 15 of each even-numbered year, the Chairman submit to the Senate Committee on Armed Services and the House Committee on Armed Services a comprehensive examination of the national military strategy. This report must delineate a national military strategy consistent with the most recent National Security Strategy prescribed by the President; the most recent annual report of the Secretary of Defense submitted to the President and Congress; and the most recent Quadrennial Defense Review conducted by the Secretary of Defense.
National Military Strategy for Cyberspace Operations (NMS-CO), December 2006	The NMS-CO describes the cyberspace domain, articulates cyberspace threats and vulnerabilities, and provides a strategic framework for action. The NMS-CO is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. The integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental to this approach.
Unified Command Plan (UCP) 6 April 2011	The UCP assigns USSTRATCOM the mission of synchronizing planning for cyberspace operations, in coordination with other CCDRs, the Services, and, as directed, other US government agencies; and executing selected cyberspace operations.

Department of Defense Documents	
Joint Operations Planning and Execution System (JOPES)	The JOPES is the Department of Defense's (DOD's) principal means for translating national security policy decisions into military plans and operations. JOPES Functional Managers grant permissions, restrict access to operation plans on the database, and perform periodic reviews of user IDs and the content of the JOPES database to ensure outdated plans and accounts are removed when no longer required.
CJCS Net-Centric Operational Environment (NCOE) Joint Integrating Concept (JIC) v1 31 Oct 2005	This document provides a conceptual look at how the NCOE will enhance the overall performance of warfighters at every level. Its focus is supporting a JTF, including the JTF commander, JTF mission partners, and warfighters at the "first tactical mile." The goal is for the entire joint force and mission partners to have the technical connectivity and interoperability necessary to rapidly and dynamically share knowledge amongst decision-makers, communities of interest, and others, while protecting information from those who should not have it—all to facilitate the coherent application of joint action. The NCOE will translate information superiority into combat power by effectively linking (both horizontally and vertically) knowledgeable entities throughout the battlespace, thus making possible dramatically new ways of operating and, by extension, decisive advantages in warfighting. The timeframe is 8 to 20 years in the future, with an illustrative focus on the year 2015.
DOD Directive 3600.01, *Information Operations*, 23 May 2011 (Secret; title and information extracted are unclassified)	Covers some of the computer network aspects of cyberspace operations, classifying them as part of IO. 3600.01 discusses "computer network operations," comprised of "computer network attack," computer network defense," and computer network exploitation," but does not discuss networks or cyberspace operations in a more holistic sense. Some further guidance may be found in the NMS-CO, but the details are not releasable at this time.
SecDef Memorandum, *Command and Control for Military Cyberspace Missions*, 12 November 2008,	Specifies that USSTRATCOM's JTF-GNO falls under the operational control of USSTRATCOM's USCYBERCOM, which directly impacts the organization of the global functional combatant command responsible for much joint cyberspace activity.

Department of Defense Documents	
DODD 3020.40, *Defense Critical Infrastructure Program* (DCIP), 14 January 2010	This Directive cancels DOD Directive 5160.54, "Critical Asset Assurance Program," January 20, 1998 (hereby canceled), updates policy, and assigns responsibilities for the DCIP, incorporating guidance from the President in Homeland Security Presidential Directive #7, December 17, 2003 to function as the Sector-Specific Agency for the Defense Industrial Base with the following responsibilities: collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector; conduct or facilitate vulnerability assessments of the sector and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources. This Directive cancels Deputy Secretary of Defense Memorandum, “Critical Infrastructure Protection Responsibilities and Realignments,” August 11, 1999 (hereby canceled) and supersedes The Department of Defense Critical Infrastructure Protection Plan, November 18, 1998 (hereby superseded), and the Deputy Secretary of Defense Memorandum, “Realignment of Critical Infrastructure Protection Oversight to the Assistant Secretary of Defense for Homeland Defense,” September 3, 2003 (hereby superseded).
DODD 3020.26, *Department of Defense Continuity Programs*, January 9, 2009	DOD policy that all defense continuity-related activities, programs, and requirements of the DOD Components, including those related to continuity of operations, continuity of government, and enduring constitutional Government, shall ensure the continuation of current approved DOD and DOD component mission essential functions all circumstances across the spectrum of threats
DODD 8500.01E, *Information Assurance*, 24 October 2002	Establishes policy and assigns responsibilities to achieve Department of Defense (DOD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

Department of Defense Documents	
DODD O-8530.01 *Computer Network Defense*, 1 January 2001	Establishes policy, definition, and responsibilities for CND within DOD information systems and computer networks
DODI O-3600.02 *Information Operations Security Classification Guidance*, 28 Nov 1995	Provides DOD-level security classification guidance relevant to some cyberspace operations
DODI 8410.02, *Network Operations for the GIG*, 19 Dec 08	Incorporates and cancels DOD chief information officer Guidance and Policy Memoranda No. 10-8460 and No. 4-8460. Establishes policy and assigns responsibilities for implementing and executing NetOps, the DOD-wide operational, organizational, and technical capabilities for operating and defending the GIG. Institutionalizes NetOps as an integral part of the GIG
JP 1, *Doctrine for the Armed Forces of the United States*, 14 May 2007, Change 1 20 March 2009	This publication is the capstone joint doctrine publication. It provides doctrine for unified action by the Armed Forces of the United States. As such, it specifies the authorized command relationships and authority that military commanders can use, provides guidance for the exercise of that military authority, provides fundamental principles and guidance for command and control, prescribes guidance for organizing joint forces, and describes policy for selected joint activities. It also provides the doctrinal basis for interagency coordination and for US military involvement in multiagency and multinational operations.
JP 2-0, *Joint Intelligence*	This publication is the keystone document of the joint intelligence series. It provides fundamental principles and guidance for intelligence support to joint operations and unified action.
JP 2-01, *Joint and National Intelligence Support to Military Operations*, 07 October 2004	This publication establishes doctrinal guidance on the provision of joint and national intelligence products, services, and support to military operations.

Department of Defense Documents	
JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*	This publication describes the process in which the adversary and other relevant aspects of the operational environment are analyzed to identify possible adversary courses of action and to support joint operation planning, execution, and assessment.
JP 3-0, *Joint Operations*, 11 August 2011	This publication is the keystone document of the joint operations series. It provides the doctrinal foundation and fundamental principles that guide the Armed Forces of the United States in the conduct of joint operations across the range of military operations.
JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I and II*, 17 March 2006	Volume I discusses the interagency, intergovernmental organization (IGO), and nongovernmental organization (NGO) environment and provides fundamental principles and guidance to facilitate coordination between the Department of Defense, and other US Government agencies, IGOs, NGOs, and regional organizations. Volume II describes key US Government departments and agencies, IGOs and NGOs — their core competencies, basic organizational structures, and relationship, or potential relationship, with the Armed Forces of the United States.
JP 3-13, *Information Operations*	This publication provides doctrine for information operations planning, preparation, execution, and assessment in support of joint operations.
JP 3-13.1, *Electronic Warfare*, 25 January 2007	This publication provides joint doctrine for electronic warfare planning, preparation, execution, and assessment in support of joint operations across the range of military operations.
JP 3-13.3, *Operations Security*, 29 June 2006	This publication provides doctrine for planning, preparation, execution, and assessment of operations security in joint operations.
JP 3-13.4, *Military Deception*, 13 July 2006	This publication provides joint doctrine for the planning and execution of military deception at the combatant command and/or subordinate joint force level.
JP 3-14, *Space Operations*, 6 January 2009	This publication provides joint doctrine for planning, executing, and assessing joint space operations.

Department of Defense Documents	
JP 3-13.2 *Military Information Support Operations*	This publication addresses military psychological operations planning and execution in support of joint, multinational, and interagency efforts across the range of military operations
JP 5-0, *Joint Operation Planning* 11 August 2011	This publication is the keystone doctrine for joint operation planning throughout the range of military operations.
JP 6-0, *Joint Communications System*	This publication is the keystone document for the communications system series of publications. This publication presents approved doctrine for communications system support to joint and multinational operations and outlines the responsibilities of Services, agencies, and combatant commands with respect to ensuring effective communications system support to commanders.

Air Force-Level Documents	
HQ USAF Program Action Directive 07-08 (Change 4), *Phase I of Implementation of Secretary of Air Force Direction to Organize Air Force Cyberspace Forces*, 20 February 2009	Organization of the Air Force's Service contribution to cyberspace operations.
Volume 1, *Basic Doctrine*	This document is the premier statement of US Air Force basic doctrine. It has been prepared under the direction of the CSAF. It establishes general doctrinal guidance for the application of air and space forces in operations across the full range of military operations

Air Force-Level Documents	
Annex 3-0, *Operations and Planning*	This document has been prepared under the direction of the CSAF. It establishes doctrinal guidance for organizing, planning, and employing air, space, and cyberspace forces at the operational level of conflict across the full range of military operations. It is the capstone of US Air Force operational-level doctrine publications. Together, these publications collectively form the basis from which commanders plan and execute their assigned air and space missions and their actions as a component of a joint Service or multinational force.
Annex 3-13, *Information Operations*	This annex establishes doctrinal guidance for information operations. More detailed doctrinal discussions of information operations concepts are explained in Annex 3-13.1, *Electronic Warfare Operations*; and Annex 3-61, *Public Affairs Operations*. The nomenclature of these publications is subject to change. Other annexes also discuss information operations as they apply to those specific airpower functions.
Annex 3-61, *Public Affairs*	This document articulates fundamental Air Force principles for conducting public affairs operations and provides commanders with operational-level guidance for employing and integrating those capabilities across the range of air, space, and information operations.