CHENNAULT EVENT #3, CYBERSPACE PROCESSES WORKSHOP AFTER ACTION REPORT

Effective Integration of Cyberspace Capabilities into Combat Operations in the United States Air Force

Abstract

This event explored the doctrine changes necessary to better enable the employment of cyberspace capabilities in conjunction with other capabilities as seamlessly as possible. In order to more effectively execute joint all domain operations or JADO, Air Force and joint doctrine should identify and incorporate processes, procedures and functions that enable the seamless integration of cyberspace capabilities into the air component.

Mr. Allen Moore, Air Force Lessons Learned, ivan.moore.4@us.af.mil
Mr. Kevin Williams, Air Force Lessons Learned, kevin.williams.111@us.af.mil

Executive Summary

Chennault Event 3 explored the integration of cyberspace capabilities into the USAF combat portfolio.[1] The first two events explored JADO operations and targeting in the next three to five years. This event, held 15-19 June 2020, at the Curtis E. LeMay Center for Doctrine Development and Education focused on identifying doctrine changes needed to improve the integration of cyberspace capabilities into air operations. The LeMay Center Doctrine Directorate was the sponsor for the event. Concepts derived from this workshop may generate an update to the *Annex 3-1 Department of the Air Force's Role in Joint All Domain Operations (JADO)* dated 01 June 2020. The event analyzed AOC processes and products while focused on cyberspace targeting, as part of infusing JADO capabilities, at scale, for a near-term interim solution. A contested environment and disrupted reachback were assumed and the workshop addressed both offensive and defensive cyberspace.

AOC changes to improve JADO integration include cyberspace SME manning levels, experience levels, and training for both the cyberspace force and other domains. The goal is to make air and space personnel cyberspace smart and make cyberspace personnel air and space smart. Furthermore, PME courses should expand content on cyberspace operations. The selection process for cyberspace SME AOC assignment should be reviewed.

Cyberspace forces should prepare for a seamless transition from competition to conflict. The Commander, AFCYBER and the JFHQ-DODIN have been delegated most of the defensive authorities from the Commander, USCYBERCOM, some of which are conditions-based authorities (CBA). The AOC needs CBA for integrated combat operations. The goal is to create a defensive cyberspace umbrella, with defensive forces from all the services and coalition performing overwatch of the systems. For offensive cyberspace, some very limited and very specific CBAs exist. Cyberspace planners require a thorough understanding of the associated battlespace via ISR products. AOC cyberspace SMEs must understand how cyberspace capabilities are accessing the targets. Often the coalition has cyberspace tools, accesses and

[1] This is the third of five scheduled events to explore doctrinal changes needed to fully implement JADO in Air Force operations. Contact Mr. Allen Moore, Curtis E. LeMay Center for Doctrine Development and Education, Air Force Lessons Learned Directorate, ivan.moore.4@us.af.mil to request the AARs for the first two events.

authorities not available to the joint force. The cyberspace force needs to mature to ensure generation of cyberspace effects in conflict at the speed needed.

During reachback-denied conditions, fielded forces will operate autonomously. The loss of reachback affects the continuity of operations, the ability to synchronize operations with other forces operating in other domains and the ability to deconflict actions. Distribution of cyberspace rules of engagement (ROE) for use during degraded communications would be very helpful. AFCYBER/CC delegation of Directive Authority for Cyber Operations (DACO) authority during periods of reachback-denied or degraded periods would also help continue defensive cyberspace actions. The operational risk derived from lowering cyberspace authorities and planning to the AOC level needs to be assessed. The defensive cyberspace mission objective should be mission assurance versus today's customer service, which is reactive. OCO forces will not have much capability in reachback-denied conditions, mostly due to inability to gain access.

The current Cyberspace Tasking Order (CTO) process is heavily focused on daily repetitive tasks involving DODIN operations. The CTO should focus on outcomes and weight of effort against these new threats and strategic messaging against adversaries. Capability to obtain authorities and perform ISR actions against targets based on dynamic opportunities should be improved. For deliberate targeting under offensive cyberspace operations, long lead times are the standard, typically around two years for strategic targets. Dynamic targeting requires a completely different response timeline. MTOs focused on campaign level guidance are needed to employ cyberspace with other capabilities. For future planning efforts, development of automated processes would greatly enhance the cyberspace workforce. MTOs could be developed to allow CCDR delegation of specific DCO and DODIN tasks to more expediently defend during conflict. An ITO at the JTF/CC level may provide better synchronization of effects across the components. There are three tasking orders across the air, space and cyberspace domains, the ATO, JSTO and CTO and three operations directives, AOD, SOD and COD. Merging these three functions into a single ITO would be a large step toward true all-domain integration. Barring an ITO, there was a suggestion for an annex to the ATO that describes associated cyberspace actions in the CTO. Who accepts the risk for MTOs or an ITO? There will likely be little integration of effects in an MTO environment, distinctly different from ITO execution.

How should cyberspace forces pre-plan for dynamic targeting? The major difference between defensive deliberate and dynamic targeting is that authorities reside with the DACO, which is currently the 616 OC. DACO authorities would have to move to the JFACC. Dynamic targeting for DCOs, DODINs and MDTs will occur when these units are pulled away from their day-to-day defensive posture to deal with a specific, immediate threat in a network or system, repair or mitigate the associated damage, perform forensics and then return to their normal functions. Currently, if a node opens up unexpectedly, the OCO, if authorized, should be able to execute a target that was already fully planned and vetted but not scheduled yet. OCO dynamic targeting on unscheduled and unanticipated targets would require employment of standard operating procedures (SOPs) and ROE such as authorities and risk assessment. A lot of doctrinal ground work is needed to identify what type of cyberspace targets would call for dynamic targeting and what would be necessary to vet the target package at the AOC (authorities, tools, etc).

Introduction

Chennault Event 3 explored the integration of cyberspace capabilities into the combat portfolio of the United States Air Force.[2] The first event, held in December 2019, sought to identify seams and shortfalls between current Air Force doctrine and the doctrine required for highly-integrated, effective JADO. The second event, held in February 2020, explored the doctrinal changes needed to better execute JADO targeting. This event, held 15-19 June 2020, at the Curtis E. LeMay Center for Doctrine Development and Education, Wargaming Directorate, Maxwell AFB, Alabama and at various sites across the Air Force focused on identifying doctrine changes needed to improve the integration of cyberspace capabilities into air operations. Fifty subject matter experts from the LeMay Center, Air University (AU) and other units across the Air Force participated. Units represented include the 26th Network Operations Squadron, Maxwell AFB, HQ Air Combat Command (ACC) A6, 16th Air Force (AF) A3/6, 616th Operations Center (OC), 390th Cyber Operations Squadron (COS), 691st COS, US Air Forces Europe (USAFE) A3, 39th Information Operations Squadron (IOS), 705th Training Squadron (TRS), 505th TRS, Shadow ShOC – N, HQ Air Force (HQ AF) A3 and the 613th Air Operations Center (AOC). Three participants from the Air War College represented AU, while sixteen personnel from various directorates represented the LeMay Center. The LeMay Center Doctrine Directorate was the sponsor for the event.[3] Due to the ongoing pandemic, only twenty-six participants were physically present. The rest participated either via TSVOIP or TSVTC. The discussions were held at the TS/SCI level.

The Chennault Event 3, Cyberspace Processes Workshop objective was to analyze AOC processes and products while focused on cyberspace targeting, as part of infusing JADO capabilities, at scale, for a near-term (three-five year) interim solution. Success occurs when cyberspace operations become a fully integrated element of our offensive and defensive capabilities. To enable the workshop to accomplish the objective, five focus areas were presented to the participants. The participants were directed to assume that operations will be contested and reachback support will be interrupted and unreliable. Each focus area was to be

[2] This is the third of five scheduled events to explore doctrinal changes needed to fully implement JADO in Air Force operations. Contact Mr. Allen Moore, Curtis E. LeMay Center for Doctrine Development and Education, Air Force Lessons Learned Directorate, ivan.moore.4@us.af.mil to request the AARs for the first two events.

[3] Concepts derived from this workshop may be included in the next update to the *Annex 3-1 Department of the Air Force's Role in Joint All Domain Operations (JADO)* dated 01 June 2020.

addressed from the perspective of defensive cyber operations (DCO), offensive cyber operations (OCO), DODIN operations and DODIN authorities.

Focus Area 1 dealt with AOC basics such as manning, equipment, systems, training, organization and structure and what changes are needed. It also addressed classification issues both for US and coalition forces that arise when cyberspace capabilities are employed. Focus Area 2 explored the problem of transitioning cyberspace operations from competition to conflict. The workshop focused on cyberspace operations authorities necessary to enable combat operations. Focus Area 3 asked how cyberspace capabilities, both offensive and defensive, should function in a reachback-denied or limited communications environment. Subject matter experts (SMEs) opined on the effectiveness of cyberspace capabilities in a reachback-denied environment. Focus Area 4 examined the problem of synchronizing cyberspace operations planning with air and space operations planning. How should the various tasking orders for air, space and cyberspace change? Finally, Focus Area 5 assessed how to develop and improve the Air Force's ability to deliver and employ cyberspace capabilities to support dynamic targeting. What pre-planned support needs to occur to make cyberspace capabilities effective tools for dynamic targeting?

The workshop was intentionally small and most of the participants were experts in the use and capabilities of cyberspace tools in offensive and defensive operations. Secure teleconferences were the primary communication method employed to discuss ideas. The LeMay Center Vice Commander and senior Doctrine Directorate personnel received the outbrief.

CHENNAULT 3.0 FOCUS AREA 1:

AOC BASICS

What needs to change in manning and training to enable the AOC to fully integrate cyberspace operations into air and space operations? AOCs have already begun to change their force structure as to how many and where cyberspace SMEs are placed. However, the workshop participants strongly believe that the critical attribute to manning the AOC is not the number of personnel. Instead, the quality of their training as well as how much and what type of experience they present is the key to fully integrated cyberspace operations. One training element currently lacking for most AOC cyberspace operators is a good understanding of how to gain appropriate cyberspace accesses and other access attributes. In addition, these personnel need to understand how capabilities in the other domains can be employed to best deliver cyberspace weapons as part of an integrated package. It was noted that no standardization exists across the services for the proper training and experience of cyberspace operators. It might make sense for cyberspace operators to cross-train with the other services. It was assessed that current training for DODIN and DCO operators was insufficient to be fully capable in the AOC. An AOC baseline for training is needed for OCO, DCO and DODIN operators. One weakness with current cyberspace operator experience and training is that cyberspace operations personnel most often reside in the tactical realm whereas AOC operations are at the operational level of war. Cyberspace operators need training and experience to be effective at the operational level. Cyberspace SMEs should demonstrate the experience to know how and where to reach back for support when able and needed. During degraded operations, cyberspace SMEs must be able to execute prepackaged targets in support of integrated operations. They also need to be aware of the authorities and restrictions that are assigned to an AOC during periods of denied communications and act accordingly. Meanwhile the rest of the AOC personnel need expanded Initial Qualification Training (IQT) content to develop an operations-level understanding of OCO, DCO and DODIN functions, actions and authorities. New Knowledge, Skills and Abilities (KSAs) need to be developed on cyberspace capabilities. The ultimate goal is to make air and space planners cyberspace smart and make cyberspace planners air and space smart. In addition to IQT, new personnel arriving at an AOC should receive a spin-up on cyberspace integration into the AOC. This could possibly occur at their ARC associated unit (such as the Battle Creek, MI unit for personnel reporting to the 603rd AOC) before reporting. Furthermore, Professional Military Education (PME) courses should expand current content on cyberspace operations. NCO

Academy, Senior NCO Academy, Squadron Officer School, Air Command and Staff College and Air War College should all provide a more robust cyberspace integration education at the operational level of war. There was a discussion about the recency of experience required for cyberspace SMEs assigned to the AOC. The cyberspace domain is changing rapidly. Outdated experience has not proved useful to current AOC cyberspace operations. How you ensure currency of experience is a question that was beyond the expertise of the workshop. But it is important that the selection process for cyberspace SMEs assigned to the AOC be reviewed and, if necessary, amended, to ensure that the candidates have the right mix of attributes and experience. Additionally, it is important to assign these SMEs to work sections where their valuable expertise will be most beneficially employed.

Even though assignment of quality personnel was deemed more important than the number of SMEs, there was consensus that not enough cyberspace operators are posted in the AOCs. Cyberspace SMEs are needed in each division from Strategy (SRD) to Combat Plans (CPD) to the Intelligence Surveillance and Reconnaissance division (ISRD) and Current Operations (COD). The Multi-Domain Warfare Officer (AFSC 13OX, sometimes called a "Thirteen Oscar"), while very valuable within an AOC, does not replace the need for cyberspace SMEs across all the divisions of the AOC.

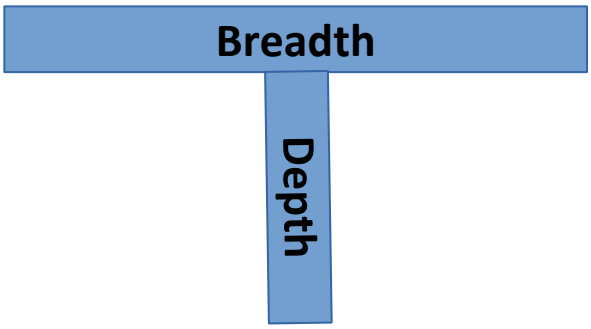

Figure 1: Cyberspace SMEs Knowledge/Experience Requirements

The cyberspace community does not have enough depth of experienced operators to provide the number and quality of manning described above across all the AOCs maintained by the Air Force. It will likely take many years to attain this level. In the meantime, it may be more effective to prioritize the AOCs that most need the top level manning just described.

There was discussion regarding an "Integrated Tasking Order" (ITO) to replace or supersede the Air Tasking Order (ATO), Joint Space Tasking Order (JSTO) or the Cyber Tasking Order (CTO). It was not clear who would generate the ITO, although it was inferred that the responsibility would reside above the AOC and cross all service components. An ITO as envisioned would likely require further analysis to determine the benefits and costs from its generation and use. Would it truly improve integration across all domains or is it simply another layer on an already complex system? Perhaps there could be, if done properly, a global ITO.

Another concept discussed was the need for a synchronization matrix at the combatant command level to depict the timing of effects delivered by the respective components to optimally synchronize in time and space. Generating cyberspace targets that cross AORs may be problematic as it is not clear who would be assigned the authority or responsibility for such actions.

There was discussion of creating an "Information Warfare" (IW) cell, likely residing at 16th Air Force but forward deployable. The cell could be manned not just with cyberspace SMEs but also Electronic Warfare (EW), IO and Signals Intelligence (SIGINT) specialists. It was noted that the 603rd AOC already maintains an IW cell manned with cyberspace, EW, IO and a limited few Space SMEs.

The workshop decided that DODIN and DCO personnel need to know what critical assets to defend before conflict occurs. If there is inadequate information available, the DODIN and DCO SMEs need to be proactive in planning to the level they need to be effective. There was some discussion whether DODIN and DCO expertise needed to reside in the Air Component, within the AOC or on the Commander Air Forces (COMAFFOR) staff. The preference leaned toward keeping the DODIN and DCO SMEs in the AOC but actively coordinating with the COMAFFOR A6 staff. This may be different across respective Air Components as their structures vary significantly. DCO and DODIN SMEs are needed in the COD and SRD. Cyberspace guidance needs to be pushed to the wings via the Air Operations Directive (AOD) and the Special Instructions (SPINS). It is clear that the Agile Combat Employment (ACE) concepts currently being developed by the air components need a well-thought out defensive cyberspace plan. It was noted that the Joint Force Air Component Commander (JFACC) lacks command and control (C2) of DCO and DOD/IN forces. That authority resides with the assigned Service Cyber Component (SCC) commander. However, the JFACC is responsible for developing and executing the Area Air Defense Plan (AADP), which necessarily includes defense of cyber systems and critical infrastructure. When responsibilities, authorities and accountability do not reside with the same commander, challenges exist.

DCO and DODIN elements/functions are not traditionally part of the AOC. While DODIN operations are not threat-specific, DCO operations are and can occur in Red and Gray cyberspace. The AOC Falconer Weapon System needs to be defended. The question was asked if the current support agreement between USCYBERCOM and the combatant commander (CCDR) adequate for executing combat operations. Does the CCDR need tactical control (TACON) of those forces? The pros and cons for both global defense and theater defense need to be compared and joint doctrine should reflect the result.

The ATO Coordinator and Non-Kinetic Effects Duty Officer (NKE-DO) have become a standard in most every AOC, especially the 603rd, 607th, 609th and 613th. There was discussion on adding a NK Operations (NKO) Coordinator to be the cyberspace effects expert throughout the ATO development process. The NKO Coordinator should operate in concert with the ATO Coordinator, should have a thorough understanding of the air plan, scheme of maneuver and how cyberspace capabilities are integrated, to aid in ensuring that integrated cyberspace effects are executed as planned. Operators should be a senior Captain or junior Major cyberspace SME.

At the wing level, the Air Force has developed deployable cyberspace Mission Defense Teams (MDTs). These teams are designed to evaluate and harden specific weapon systems (e.g. F-16, F-35, etc) from cyberspace vulnerabilities. They develop a deep understanding of all the systems associated with their weapons system in order to recognize cyberspace vulnerabilities and develop necessary strategies to minimize or eliminate the threat.[4]

The classification of cyberspace effects, access and network tools are a real barrier to the integration of cyberspace operations into the air operations plan. Lack of understanding breeds distrust and secrecy inside the AOC inhibits integration. When coalition forces are added to the AOC planning process, classification and releasability becomes an issue that makes integrating cyberspace operations difficult. A thorough security classification guide (SCG) for cyberspace needs to be developed. Current SCGs for cyberspace operations tend to be classified heavily TOP SECRET and generic, limiting their usefulness. Artificial Intelligence (AI) capabilities were discussed to review documents and other products to determine classification levels and releasability but there was consensus that the process would still require a human in the loop. The best place to solve releasability problems before any conflict occurs is at USCYBERCOM. Cyberspace capabilities and effects tend to be at the TOP SECRET level. A way to integrate coalition forces and AOC personnel is to build a TOP SECRET work section, perhaps elevated, on the AOC COD floor. There is an additional need to explore multi-domain and coalition systems for available capabilities. Many partners use common hacker tools that are found in the commercial market. These should not be classified. The typical Foreign Disclosure Officer (FDO) in the AOC is not trained and lacks experience in cyberspace capabilities to properly understand the releasability to our coalition partners. The foreign disclosure process, though not new, is very cumbersome and likely to cause delays. Stripping the intelligence source(s) from the cyberspace documents would allow for lower classification levels of cyberspace capabilities and effects. Also breaking any link of effects to specific targets may allow for releasability. Addressing the review and approval process before conflict will help enable most releasability decisions to be made early in the planning process. Cyberspace capabilities registry does exist at the unclassified level and assists in easing classification burdens.

[4]ACC is currently standing up an MDT to help defend the AOCs.

FOCUS AREA 2:

TRANSITIONING FROM COMPETITION TO CONFLICT

How can cyberspace forces prepare for a seamless transition from competition to conflict? In competition cyberspace effects are rarely integrated into a force package. Instead the actions and targets stand alone, since competition does not generate force packages. The time required to perform the target development is significant and can take months or even years. Its use is also very deliberate. Cyberspace access ports are often compromised when acted on, therefore any actions during the competition phase must weigh the benefit of the effect versus the loss of access, i.e. intel gain/loss determination. Timing is important but not critical. In competition, authority levels are not critical due to the standard timeline for requesting approval to plan or execute a cyberspace effect. Once competition transitions into the conflict phase, it is expected that current planning or timing process will and must adjust to meet the demands of the conflict phase

In this focus area, the workshop was asked to consider what authorities are required to target and generate cyberspace effects.

The USCYBERCOM Commander has delegated the majority of the defensive authorities to the AFCYBER Commander and JFHQ-DODIN. The cyberspace community has developed a conditions-based authorities (CBA) approach for delegation of execution of specific capabilities. AOC planners should assess the mission risk and the cyberspace effects that the CBA can assist with. That risk needs to account for operating in a reachback-denied environment. For DCO and DODIN actions, the workshop identified a need for access to other service networks, coalition networks, host nation network, commercial networks and the logistics network. Waiting until conflict to grant those authorities is a gamble, because it takes time to gain adequate situational awareness with the network in order to identify and repair network or system vulnerabilities. In competition, the DCO should be performing vulnerability assessments for the theater and assisting with identifying indicators and warnings. To do this requires a very good understanding of the operational plan, the theater and potential adversaries. It is not likely that AFCYBER has the level of knowledge and understanding of various theaters. This lack of understanding may result in defensive cyberspace capabilities being underutilized. The goal is to

create a defensive cyberspace umbrella, with defensive forces from all the services and coalition partners performing overwatch of the systems.

For offensive cyberspace, limited and specific CBA does exist. Often, the CBA is based upon a specific trigger. The 616th OC sometimes executes specific cyberspace action for the AOC. During operations, cyberspace SMEs in the COD, SRD and Master Air Attack Planning (MAAP) cells need to be aware of the cyberspace target packages plans to access a system. Kinetic operations may inadvertently destroy those accesses. If discovered, an opportunity cost must be determined with the appropriate decision made based on risk factors. Either strike the target kinetically and lose the capability to affect cyberspace targets that were using that access or make the determination to not strike it. Access points or locations should be put on the Restricted Target List (RTL) to avoid inadvertent damage. If they are not, the JFACC should be aware of the cost of losing that access point. Kinetic actions may also be used in support of cyberspace actions by destroying the access point after the cyberspace event occurs, thus preventing the adversary from using cyberspace forensic tools to determine the source and how access was gained.

USCYBERCOM has attached a Cyberspace Operations – Integrated Planning Element (COIPE) to each geographic commander. Each COIPE sits at the Joint Force Commander (JFC) level. The element serves as a support planning element for all offensive cyberspace planning and integration of cyberspace targets. It advocates for cyberspace equities in the geographic (GCC) or functional commands (FCC). Furthermore, it also advocates for the GCC or FCC at USCYBERCOM. It keeps the CCMD informed about defensive cyberspace issues in the command.

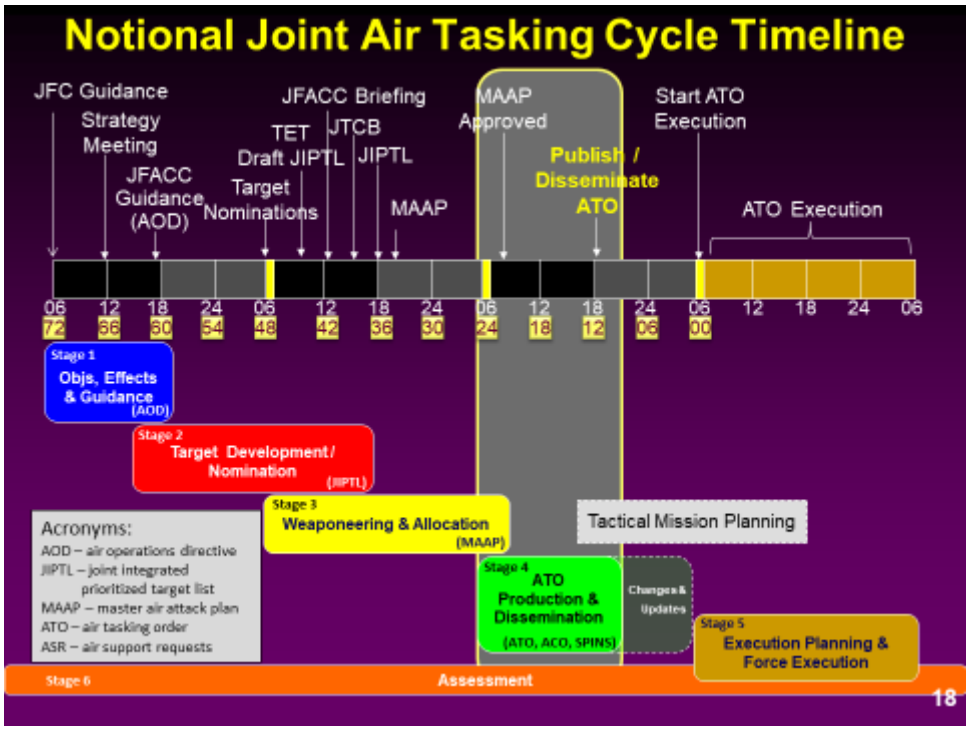

Figure 2: Joint Air Tasking Timeline (Source 505th CCTS)[5]

The objective is to provide one single holistic viewpoint on cyberspace planning and defensive issues for the CCMD. Since it resides with the JFC, there should be a liaison element attached to the AOC. The COIPE leads the operational cyberspace planning for the GCC or FCC. Through the OC, AFCYBER does the same thing for DCO forces. Unfortunately, so far AFCYBER planners have not yet demonstrated a strong understanding of the GCCs and FCCs battlespace. Also, the operational planners at the GCC and FCC do not understand the full complement of cyberspace capabilities. Theater planners must have a thorough understanding of the associated battlespace or planning will be incomplete, assume capabilities not available or may expend limited resources. Planners may not fully vet adversary cyberspace dependencies and weaknesses. Defensively, thorough mission analysis will aid the DCOs. ISR products help project what cyberspace targets the adversary is after. This will help DCOs marshal their resources. The MDTs, mentioned earlier in this report, need to know this information as well with respect to the weapon system they are defending. MDTs must have a thorough understanding of the cyberspace vulnerabilities of the weapon system. This will require a strong relationship with the weapon system's System Program Office (SPO).

Successful cyberspace operations require a robust targeting process. Targets require engagement even when reachback is denied. To be effective, cyberspace SMEs in the AOC must understand how cyberspace capabilities are accessing targets. If access is lost, the SMEs must quickly determine how to regain it. Access planning needs to extend to the AOC for each Air Component cyberspace target. Target planning has two elements. First, target analysis is done

[5]This figure was brought forward from the Chennault 2.0 AAR

at the appropriate Joint Force Headquarters (JFHQ)-Cyber. Once complete, the target package is sent to USCYBERCOM to be racked and stacked with all the other cyberspace targets. The AOC gets cyberspace target information from the COIPE. It is important for the AOC to maintain a strong connection with the COIPE throughout the conflict and integrate the element into the AOC planning process. On the service side, each theater AOC needs a mature relationship with the 616 OC to ensure a robust cyberspace defense. The JFACC sits on the JFC's Joint Cyber Center (JCC). This is the mechanism by which the CCMD plans and integrates cyberspace operations into full spectrum military operations. The JCC also makes requests for cyberspace operations support if the CCMD lacks authority, information, intelligence, capabilities or the capacity to conduct cyberspace operations. Since the COIPE is also part of the JCC, the JFACC can use this venue to inform the COIPE about AOC cyberspace operations requirements.

Coalition forces can also play a role in offensive cyberspace operations. Coalition forces may have cyberspace accesses not available to the joint force. They may have tools and authorities not available to the joint force. Coalition forces and the joint cyberspace forces need to ensure they coordinate, deconflict and plan operations, especially if the joint combined force resources are limited.

The bottom line is this: the cyberspace community's ability to transition from competition to conflict is problematic. Target development is slow and there are no current mechanisms in place to speed them up. Access for targets being developed are not determined until late in the planning process. Majority of the planning level is done above the AOC, removing the valuable knowledge of targets and access points for cyberspace SMEs. The COIPE and MDTs are in their infancy. Over time and with some maturing AOCs may be able to plan with cyberspace capabilities at the speed required. Currently, cyberspace forces' observe, orient, decide and act (OODA) loop is slow and bureaucratic. It does not match the Air Force culture of centralized control, decentralized execution. For purposes of air and space operations, it also misaligns authorities, responsibilities and accountability. The advantage of the current cyberspace force structure is that it maintains a strong unity of command with a global reach. However, if reachback is denied, the cyberspace processes become even more problematic. All of this needs to be resolved soon in order for cyberspace forces to be able to shoulder significant portions of the air and space battle.

FOCUS AREA 3:

CYBERSPACE OPERATIONS IN A REACHBACK-DENIED OR DEGRADED ENVIRONMENT

The joint publication 3-12, *Cyberspace Operations*[6], does not define reachback for the cyberspace community. There is a definition in the *DOD Dictionary of Military and Associated Military Terms*[7] for reachback but it is not satisfactory for the purposes of the workshop. The workshop described the reachback-denied condition as the following: the fielded forces are on their own in theater. They can communicate with the coalition but are unable to communicate beyond the joint operating area (JOA) or even to higher HQs within the CCMD's area of responsibility (AOR). Specifically, it was suggested that a reachback-denied condition occurs when USCYBERCOM cannot access the internet, cannot communicate with the JFC and the JFC cannot communicate with fielded forces. When reachback is denied, the AOC is unable to communicate with multiple critical nodes within the planning and execution system. A degraded environment occurs when some or all of these conditions occur intermittently, causing disruption to combat operations.

The loss of reachback affects the continuity of operations, ability to synchronize operations with other forces operating within other domains and the ability to deconflict actions and effects. The AOC will be unable to receive instructions or to synchronize and integrate cyberspace actions from USCYBERCOM or from the JFC. Furthermore, proper authorities may not be established to perform cyberspace operations on friendly and adversaries' networks. Planners may be unable to develop target packages for future operations. Whether that is a serious problem will depend on how long the reachback-denied situation exists. Reachback forces should continue to develop existing target packages, with the understanding that future targets cannot be nominated by the AOC.

The workshop was asked to identify what cyberspace effects the AOC needed to be able to generate in a reachback-denied environment and compare them against what the workshop assessed the AOC could do.

---

[6]JP 3-12, dated 8 June 2018
[7]Dated June 2020

A possible characteristic of degraded reachback for cyberspace operations is that DCO will likely be more effective than OCO. There are global concerns that cannot be addressed when reachback is degraded or not possible. Participants discussed an aid or tool for the AOC and fielded units would be the development and distribution of cyberspace rules of engagement (ROE) during degraded or denied communications. They suggested the ROE could consist of "if, then" statements to guide the AOC or fielded forces. AFCYBER/CC delegation of Directive Authority for Cyber Operations (DACO) authority during periods of reachback-denied or degraded periods would also help continue defensive cyberspace actions. SPINS could serve as a method to deliver the ROE to the fielded units. It was noted that in some circumstances the databases from which patches for the networks reside may be in the CONUS. Inability to quickly patch networks in an extended reachback-denied period would increase the cyberspace vulnerability of the AOC. Since most defensive capabilities involve commercial off-the-shelf technologies, DCOs and MDTs during conflict should be able to access patches directly or maintain an internal inventory, thus reducing network and system security delays.

Some questions need to be asked and answered. The associated operational risk needs to be assessed. There is an inherent struggle in the cyberspace community between unity of action and marshaling strategic resources for global use, and the Air Force method of decentralized execution, pushing authorities and capabilities down to the lowest possible level. In peacetime and in the competition phase, unity of command is the preferred method. However, there are concerns when transition to conflict occurs. Pre-planning for CBA and a robust means to access the database will be required. For defensive operations, mission task orders (MTOs) from the AFCYBER/CC[8] would work well. Those MTOs could be posted in the AOD for fielded forces.

It was noted that the networks the DCOs, DODIN and MDTs are protecting may be vulnerable to SCADA system attacks.[9] Possible vulnerabilities should be identified, analyzed and assessed. MDTs and DCOs lack operational expertise and experience in working together. Exercises are needed to integrate these entities into a strong cyberspace defense force. Furthermore, defensive cyberspace forces are not provided situational awareness of the cyberspace within their AOR. This lack of cyberspace situational awareness will lead to gaps in understanding the activity within the networks. It is important that the AFCYBER/A2 and ISRD capture and consolidate cyberspace intelligence for the Air Component. However, they rely on cyberspace operators to push the required information. The cyberspace community needs to work on improving and tailoring intelligence for fielded cyberspace forces.

A culture change is needed in the cyberspace defense community. The defensive cyberspace mission objective should be mission assurance, which employs a proactive defense posture versus today's customer service, which is reactive. A mission assurance model would enable mission owners to perform a risk assessment of their networks and systems. It was noted by the participants that that the Cyber Security Support Providers (CSSPs) are not being held

[8] It is possible that cyberspace-directing MTOs could be generated by the AOC.

[9] Supervisory control and data acquisition – SCADA refers to ICS (industrial control systems) used to control infrastructure processes. Refer to scadasystems.net for a general description of these types of systems.

accountable. These professionals are responsible for maintaining a healthy network, identifying and preventing intrusions and other cyberspace incidents. However, many CSSPs are not proactive in protecting their networks. More often, they are reacting when incidents occur. DCOs and DODINs find themselves often doing the CSSPs' functions. The workshop recommended that higher quality CSSPs be aligned with DCOs, DODINs and MDTs. This collusion could result in a layered, multi-tiered defense of the Air Force networks and systems. Doctrine should address cyberspace accountability.

It was noted by the workshop that DCO operators are reactive by nature. To be proactive, they need to posture themselves in both the logical and physical realms. This is done by positioning both human operators and automated systems in the cyberspace loop. Reactions could occur in real time if actions are triggered by specific conditions being met.

OCO forces are performing actions designed to generate the following effects: deny, degrade, disrupt, destroy and manipulate adversary actors and systems. These are very complex actions. The workshop did not believe that offensive cyberspace actions can occur in a reachback-denied environment. OCO is mostly conducted remotely. The biggest problem is access. It is not assured and some strike packages are built with secondary or tertiary access points. Generating access from the AOC under reachback-denied conditions would be very difficult. Synchronizing cyberspace actions with a strike package to generate a coherent effect would be equally difficult.

Even if the AOC was able to generate cyberspace target packages, including access, in a reachback-denied environment that is not enough. The cyberspace SMEs in the AOC would have to be able to accurately calculate the probability that the use of the access point would be detected, whether the action was attributable and a whole range of risk conditions. Then they would have to be able to assess, at the strategic level, whether the risks are acceptable. Unless training and education requirements change, AOC-assigned cyberspace SMEs may not be able to represent their community properly.

Collecting battle damage indicators (BDI) and performing battle damage assessments (BDA) is difficult for the AOC cyberspace SMEs and ISRD to properly execute. Feedback is usually provided via chat channel or a report.

Bottom line: if the AOC is operating in a reachback-denied or degraded environment for an extended period, cyberspace operations are going to fall in frequency and effectiveness. Offensive cyberspace is most severely impacted. Defensive cyberspace is also affected but not as severely. There are some actions the Air Force can take to improve capability but the improvements are on the margins. Planning and executing both offensive and defensive actions are extremely difficult without reachback access.

FOCUS AREA 4:

SYNCHRONIZING PLANNING

So what do MTOs look like in cyberspace? There is a need to adjust daily operations in a denied-communications environment. The current CTO process is heavily focused on daily repetitive tasks involving DODIN operations. Per 616 OC personnel, 99% of the CTO guidance involves routine daily DODIN operations tasks, typically a CSSP responsibility for defending the network. Much of this could be automated with more focus on unique tasking for intelligence-related actions against emerging threats and development of tactics, techniques and procedures (TTPs) against threats. The CTO should focus on outcomes and weight of effort against emerging threats and strategic messaging against adversaries. The steady state planning effort likely would vary considerably during full-scale conflict.

Currently, much of the cyberspace tasking processes involve high-level guidance and are not tasking DODIN desired outputs. Capability to obtain lower-level authorities and perform ISR actions against targets based on dynamic opportunities is under-developed. For deliberate targeting under offensive cyberspace operations, long lead times are the standard, typically around two years for strategic targets. While typically not an issue during peacetime, dynamic targeting requires a completely different response timeline. There has not been an attempt to create MTOs focused on campaign level guidance to employ cyberspace with other capabilities. Cyberspace considerations are examined in operational plans, campaign Plans, operation orders and air component support plans, with a five-year outlook. There are cyberspace operations planning considerations within the current ATO cycle with distinct touch points in the SRD during the Air Operations Directive development and Joint Air Operations Plan, the Combat Plans Division during MAAP formulation as well as during creation of the Joint Integrated Prioritized Target List (JIPTL). The 616 OC supports CCMDs throughout these planning steps. Additionally, the Cyber Threat Operations Center (CTOC) coordinates directly with AOCs on specific threats.

Current C2 and support constructs are not standardized between domains. This would be a beneficial way ahead for the JADC2 structure. Additionally, JFHQ-C service components conduct their support to combatant command using different processes. As integration continues to advance, common terminology is taking root and varied domain entities are learning how to work within the planning cycle timelines to synchronize effects. Changes in planning cycles

may not be required; instead, further education and training on capabilities and processes across the varied domain entities can increase synergy of effects. Revising curriculum in AOC training, upgrade training and PME/PCE courses will help raise knowledge levels and encourage further interaction to better leverage existing capabilities.

For future planning efforts, development of automated processes would greatly enhance the cyberspace workforce. Inputs could be ingested much faster to develop better CTO outputs and may help vector the weight of prioritization in the CTO, MTOs and potentially ITO. By automating many of the large volume, repetitive tasks that are cognitive in nature, more focus could be placed on the reactive items requiring immediate focus. MTOs would be developed to allow CCDR delegation of specific DCO and DODIN tasks to more expediently defend during conflict. Additionally, there was considerable discussion of the benefit of an ITO at the JTF/CC level to provide better synchronization of effects across the components. The AOD has been used to provide MTOs to subordinate units and may be an option to extend cyberspace guidance as well. Designating alert DCO units may prove beneficial to countering evolving adversary threats.

There was discussion on who accepts the risk for MTOs or an ITO. Within the OCO realm there likely will be little change from current procedures due to the nature and sensitivity of these actions. There may be some capability for a mission profile planner to nominate OCO actions typically depicted on a CTO to an ITO to further synchronize effects provided target development has been conducted and appropriate authorities are in place. Combatant commands will need more forces focused on target development to make this possible. For DCO/RA, during conflict the delegation would likely be directed to the CCDR/J3. Conversely, DCO/DODIN risk to terrain falls to the mission commander but may need further delegation. In the AMT realm, development of a CONOP for more opportunistic cyberspace targeting may prove fruitful. There will likely be little integration of effects in an MTO environment, distinctly different from ITO execution.

For future execution, MTOs will likely provide far less prescriptive guidance than the current CTOs. An ideal format for future MTOs would be to provide guidance, authorities and timelines in line with the planned ITO for all domains. These MTOs would be broadly described in the AOD to give guidance and flexibility to commanders for defensive actions during time of need, "go do" actions, identify risk acceptance levels, and delegated authorities (like recon and maneuver) enabling lower level teams to act quickly and accept risk. CYBERCOM is currently examining these constructs. Another potential action may be to create a cyberspace annex to the ATO, similar to the Reconnaissance, Surveillance and Target Acquisition (RSTA) Annex. This could provide a standardized place for broad tasking instructions that could cover an extended period. During conflict, risk acceptance needs to be delegated to the lowest possible level for DCO and DODIN actions. In general, an MTO would be ideal to continue day-to-day operations in time of denied communications, whereas an ITO is essential to integrate effects.

So how does the JFACC assess DCO actions and effects? Whatever assessment is done, it usually occurs above the JFACC, either in the JFC or, more likely, at the 616th OC. The JFACC has to accept the risk of adversary action in the network and systems employed. The DCO's actions can be assessed but the desired effect is very difficult to assess and is likely unknown. In

the future, AI may prove capable of improving DCO/DODIN assessments and give the JFACC a better indicator of adversary activities in the network. On the OCO side, it is extremely difficult to assess the effect of cyberspace actions. Most collection actually occurs outside the cyberspace domain. The OCO battlespace damage assessment (BDA) plan exists in the Advanced Target Development (ATD) plan and in the strike plan.

Synchronizing planning requires common terminology. There are three tasking orders, the ATO, STO and CTO and three operations directives, AOD, SOD and COD. Merging these three functions into a single ITO would be a large step toward true all-domain integration. However, a lot of important hurdles exist. Some are described elsewhere in the report. Doctrine planners need to decide if the benefits of bringing together all domain taskings into a single function outweigh the costs to execute operations. The workshop was unable to fully answer that question. Barring an ITO, there was a suggestion for an annex to the ATO that describes associated cyberspace actions in the CTO. MTOs for cyberspace operations also have the potential to improve integration as long as the attributes of the MTOs provide "go do" instructions, provide acceptable risk levels, and are able to be executed at the necessary speed to be part of an ongoing strike package. During conflict, risk acceptance needs to be at the lowest possible level. MTOs are great for day-to-day cyberspace operations but may not work so well for integrated operations. Whatever ties domains together is valuable, as long as capability, flexibility and timeliness of combat actions are not lost in the change.

It was mentioned earlier that authorities need to be assigned at the lowest level. At whatever level that is, the associated commander must also receive guidance on the allowable risk level the commander can accept. The attributes of tools associated with the allowable risk at the JFACC level, for example, may be low tools that can be used for ISR collection or to probe the adversary's networks and systems. They may also scout the cyberspace terrain. ROE would be necessary that matches the risk level allowed. One important attribute will likely be that the tools are not able to intersect with other domains.

FOCUS AREA 5:

DYNAMIC TARGETING

The Workshop was asked how do and should cyberspace forces pre-plan for dynamic targeting. The workshop observed that most DCO, DODIN and MDT actions are dynamic targeting. The DODIN forces take actions but they are not really targeting. They are merely proactively protecting the network. DCO targeting is usually tactical but there are dynamic targets DCO could engage. The best comparison between DCOs and air operations is the Defensive Counter-Air (DCA) mission. DCOs seek out targets of opportunity. The major difference between deliberate and dynamic targeting is that authorities reside with the DACO, which is currently the 616 OC. In order to affect dynamic targets, DACO authorities would have to move to the JFACC. Defensive operations are mostly an established process. To respond to a target in the network or system, defensive cyberspace forces should plan how to mitigate the targets effects, plan for recovery of network or systems and follow guidance and ROE found in the MTOs. Time-sensitive targeting (TST) can occur when a known indicator is triggered. The response should be immediate.

The AOC should develop an All Domain Defense Control Plan. This plan should identify units that will defend against cyberspace actions. The plan should be coordinated with AFCYBER. Dynamic targeting for DCOs, DODINs and MDTs will occur when these units are pulled away from their day-to-day defensive posture to deal with a specific, immediate threat in a network or system. The units will deal with the threat, repair or mitigate the associated damage, perform forensics and then return to their normal functions. Defensive actions are of two types, block IP addresses or investigate and categorize incidents. DCOs normally do not address every incident. Incidents are prioritized by the DCOs using their discretion as to where to apply their resources.

Currently OCOs do not do dynamic targeting. The workshop was asked if OCOs could strike an unanticipated target. If a node opens up unexpectedly, the OCO, if authorized, should be able to execute a target that was already fully planned and vetted but not scheduled yet.

But, if OCOs conducted dynamic targeting on unscheduled and unanticipated targets, workshop attendees were asked how they would accomplish this. The OCO would require some kind of standard operating procedure (SOP) to employ. There would have to be mission planning – whatever is determined to be the minimum required for execution. It would have to fit inside the

AOC's 24-hour execution window and still allow time for execution. There likely would be ROE such as authorities and risk assessment. Perhaps the final target execution to provide to the OCO would be in the form of a 9-line, a familiar form for air operations, used in dynamic and TST targeting. Given how demanding cyberspace planning can be, it is probable that some ground work on the target would have to have been done before the execution period. There are a lot of humans in the normal planning loop that is now being compressed into the minimum necessary to build a dynamic target package and execute it. A lot of doctrinal ground work is needed to identify what type of cyberspace targets would call for dynamic targeting and what would be necessary to vet the target package at the AOC (authorities, tools, etc). Dynamic targeting would most definitely require automation to take the place of many of the humans. A registration of cyberspace targets across multiple agencies would be useful to inform AOC targeting plans. Also the creation and maintenance of Future Response Options Matrix for offensive cyberspace operations would be very useful. Approved by USCYBERCOM, it would be conditions-based.

Bottom line: the Air Force needs to determine what would be gained by conducting dynamic cyberspace targeting and the associated cost in manpower and resources. Then they would have to convince USCYBERCOM that the benefits of dynamic cyberspace operations offset the cost of higher risk to global capabilities.

Traditionally, the fledgling cyberspace forces have operated and planned against strategic targets. They have routinely focused against strategic centers of gravity (COGs) whereas the AOC requires them to tackle operational COGs. It was also noted that often AOCs want the OCOs to strike operationally high-value targets that require exquisite planning that can cross years to execute. The OCOs and AOCs need to identify low-hanging fruit that will assist the AOC to execute its mission and not demand extensive cyberspace planning for the cyberspace effect to be generated. This is especially true for dynamic targeting to occur. Planning operational targets of value to the AOC is a fairly new requirement. The Air Force needs to provide, train and equip cyberspace forces to be able to converge against operational targets in a relevant time frame. It was noted that cyberspace forces of all the services are becoming less and less dependent upon Title 50 capabilities. More Title 10 capabilities are coming on line requiring a rapid change to training.

In reality, today the vast majority are focused on competition targets and the rest are addressing strategic targets. Few resources remain for planning of operational targets in preparation for a possible conflict. Even if the Air Force is truly able to execute JADO, cyberspace capabilities may not be there for several years. It will take a while to grow and age the force such that it is capable of planning and executing cyberspace targets. But the Air Force needs to be ready for that day today. Laying the ground work now will pay huge dividends in 3-5 years. In addition to a capacity gap, there exist training, exercise, process and organization gaps that need to be addressed. Also, operators from other domains need to be educated on cyberspace operations, both offensive and defensive.

In the Chennault 2.0 AAR, we talked about the possibility of standing up a non-kinetic football element that, like the current ATO coordinator, moves from the SRD to the CPD and ISRD and the COP in conjunction with the current ATO cycle.

The "ATO Football" Team concept is a simple variation of how the AOC operates to day. The group recommended a team, led by a Thirteen Oscar, stay with the ATO from strategy to assessment. The team construct is described in **Figure 3**. The larger the team the larger the ATO it can effectively support. Importantly, the team needs to be led by a Thirteen Oscar and needs to include other domain experts (especially space, cyberspace and the electro-magnetic spectrum (EMS). The objective of the team is make sure the strategy and planners' intent gets implemented on the combat operations floor. The ATO football team must integrate with the domain duty officers (Four Horsemen) on Combat Ops Floor. Planners would require proficiency on the 6+ databases and systems used in the ATO process. Every domain in the JADO would be represented.

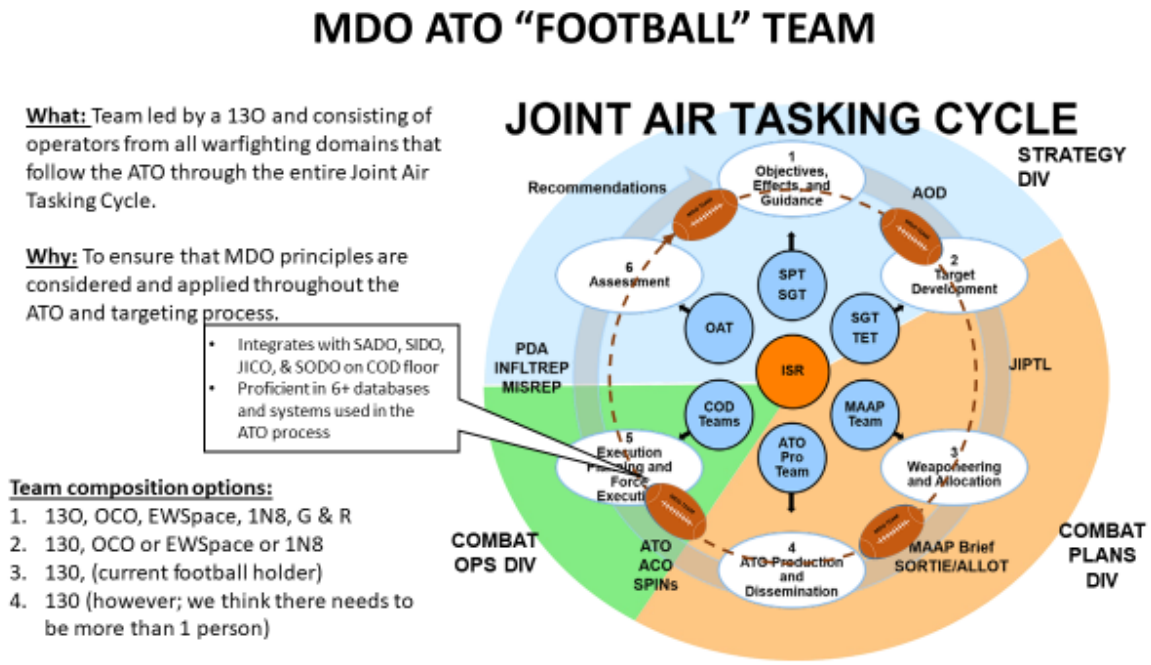

Figure 3: Chennault 2.0 Workshop Concept of ATO Planning and Execution[10]

Finally, cyberspace forces could be generated by the Air Force that are organized, trained and equipped to deliver Air Force-specific operational effects. For example, a team could be stood up whose primary objective is to de-integrate an adversary's integrated air and missile defense system. Other services are creating similar types of cyberspace forces to meet their domain-specific needs, not currently met by the strategic force. The ability to execute cyber-based ISR at the AOC against AOC targets, the ability to have dedicated cyberspace forces that the AOC controls and maintaining cyberspace tools in the AOC that enable the strike of operationally-

[10]This figure was brought forward from the Chennault 2.0 AAR. Only team compositions 1 and 2 would work.

relevant targets appears to be something worth studying and possibly funding. Until then, AOCs will likely have to learn how to be successful without significant offensive cyberspace support.

Way Ahead

Chennault 3.0 was the third in a series of events intended to inform future JADO doctrine. The intent is to use each subsequent event as a building block for future events. As such, The LeMay Center will execute Chennault 4.0 in the August or September 2020 time frame. It is currently planned as an event to address and design an ITO as outlined in the Annex 3-1. All lessons will culminate in a major wargame during the summer of 2021. The goal of the wargame and the Chennault series are to identify alterations to be made to Air Force doctrine for JADO. The Air Force processes, products and organization that currently exist need modifications to facilitate more synergistic and integrated all-domain combat operations.