The Joint Force Air Component Commander and the Integration of Offensive Cyberspace Effects

Power Projection through Cyberspace

Capt Jason M. Gargan, USAF

Cyberspace can provide great opportunities to assist the joint force air component commander (JFACC) in the field. This article explains how the JFACC can best understand, integrate, and command and control (C2) offensive cyber operations into a war plan to produce effects necessary for the mission. The idea of a few keystrokes neutralizing the enemy's integrated air defenses will mesmerize just about everyone. Instead of employing a pricey kinetic weapon against a target, a cyber operator can simply take it out at the proper time and place—in theory. Offensive cyberspace operations have the potential to provide these types of power-projecting effects in the battlespace, but how can the JFACC gain access to, integrate, and C2 offensive cyberspace operations?

The direct connection between those operations and the JFACC continues to be a substantial focus area. This article proposes a solution—one that will work within the constraints of the 2013 Joint Staff Execution Order on "Implementing Cyberspace Operations Command and Control." This order defines two C2 frameworks that are important to comprehending the rest of this study: the direct support model (the current model) and the operational control (OPCON) model, both of which were defined as part of a transitional approach to allow for the maturation of command relationships, authorities, and buildup of operational capacity.

In the direct support model, integration of offensive cyberspace operations is best understood by examining forces presented in the cyberspace domain as a peer component to the air, land, and maritime components. That said, the air component is supported by offensive cyberspace operations forces from the cyberspace component (currently OPCON to the combatant-command-aligned Joint Force Headquarters–Cyberspace). These combatant-command-aligned offensive cyberspace operations forces offer new opportunities for the JFACC to achieve air component effects and objectives in the battlespace. Understanding OPCON of cyberspace operations forces is key for all components within a joint force because the latter have objectives that could be attained through the offensive cyberspace operations mission area. Ultimately, this means that the JFACC does not own (and will not

own) offensive cyberspace forces (even in Air Force uniforms) but will be supported by what eventually will become the joint force cyberspace component commander (in the OPCON model).

To effectively integrate offensive cyberspace operations, the JFACC must be familiar with available cyber forces, cyberspace guidance, and the proposed liaisons outlined in this article. Cyberspace planning and execution factors will not be foreign to the JFACC. Cyberspace planning doctrine is modeled after air planning doctrine but incurs its own domain-specific planning, target development, and execution considerations. The article further explains the importance of forces, guidance, and liaisons to show how offensive cyberspace operations can be integrated into the rest of the air campaign.

Cyberspace Guidance

To fully integrate offensive cyberspace effects, a JFACC must grasp the cyberspace capabilities that need to be planned, coordinated, and executed to support the joint air operations mission. Where and when does the JFACC require some degree of cyberspace superiority? The classic answer to this question is, "It depends." Planning factors include the phase of the campaign, the JFACC's objectives that support the overall mission priorities of the joint force command, and the combatant command's available cyber forces. Cyberspace operations must be cohesively fused into the air component's planning efforts if they are to benefit its mission. Consequently, the JFACC should create operational-level guidance for supporting cyber forces. According to Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations*, "Proper recognition and integration of these [cyberspace] force capabilities during planning and execution is essential."[1]

The operational-level guidance on offensive cyberspace is issued through the standard means for joint air operations—the joint air operations directive and the air operations directive—thus ensuring that it receives proper attention from the JFACC and that the requested effects either fulfill or support the overall objectives of the air component. After the requested effects become viable for cyberspace action (i.e., access exists, authorities are granted, capabilities are matched to the target, and forces are available), the air operations directive must include the appropriately worded tactical objectives, tasks, and measures of performance and effectiveness for the intended time period of execution. In some cases, the task will support a tactical objective that already exists—that is, the objective includes tasks that could be executed by airborne assets as well as offensive cyberspace assets. By including the planned cyberspace effects in the air operations directive, the JFACC will receive feedback through the normal cycle processes of joint targeting, thereby integrating offensive cyberspace operations into the JFACC's standard preexisting processes. Although an effect through offensive cyberspace would likely be executed closer to the onset of conflict, that action does not prevent air component planners from thinking of effects that could be delivered as options to deter an adversary from increasing aggression.

One planning consideration regarding the use of cyberspace rather than airborne assets is the lead time necessary to generate intelligence for the offensive cyberspace effects. Target development should be requested much earlier than that for a traditional airborne target and should have a longer-term focus. More often, full target development takes weeks, months, or years instead of days.

Cyberspace Forces

As mentioned, knowledge of available forces and their organization is a major part of the planning process and the integration and C2 of cyberspace operations. Depending upon the situation, the JFACC can leverage joint cyber forces to provide offensive effects in support of the air component's objectives. The current C2 framework—the direct support model—has key offensive cyberspace operations organizations that can coordinate and conduct those operations: the combatant command's joint cyberspace center, Joint Force Headquarters–Cyberspace, and the offensive cyberspace operations tactical units, including the combat mission team and combat support team (see the figure below). Each JFACC should take time to study the progress that his or her respective combatant command has made with respect to establishing the joint cyberspace center's mission.

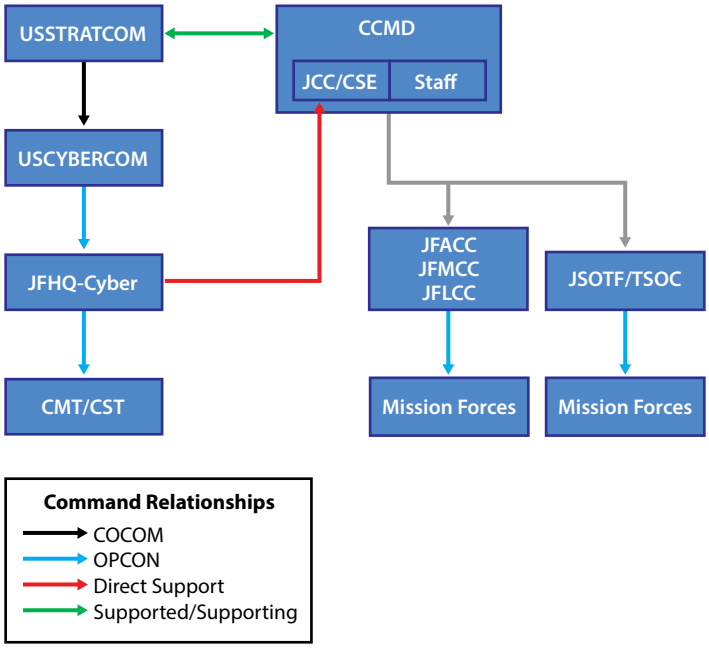


Figure. A combatant command's offensive cyberspace forces in the direct support model

USSTRATCOM - US Strategic Command
USCYBERCOM - US Cyber Command

JFHQ-Cyber - Joint Force Headquarters–Cyberspace
CMT/CST - Combat Mission Team / Combat Support Team
CCMD - Combatant Command
JCC/CSE - Joint Cyberspace Center / Cyberspace Support Element
JFACC - Joint Force Air Component Commander
JFMCC - Joint Force Maritime Component Commander
JFLCC - Joint Force Land Component Commander
JSOTF/TSOC - Joint Special Operations Task Force / Theater Special Operations Command
COCOM - Combatant Command (Command Authority)
OPCON - Operational Control

Joint Cyberspace Center and Cyberspace Support Element

The joint cyberspace center is responsible for the three lines of cyberspace operations: Department of Defense (DOD) information network operations, defensive cyberspace operations, and offensive cyberspace operations, including regional, national, and allied capabilities supporting the combatant commander's objectives. Additionally, the center is tasked to coordinate, integrate, and synchronize cyberspace operations and effects with those operations in the other war-fighting domains within the combatant command. The joint cyberspace center receives direct support from US Cyber Command's (USCYBERCOM) cyberspace support element. Each combatant command's joint cyberspace center has an associated cyberspace support element that fulfills the direct-support relationship and reaches back to USCYBERCOM.

Joint Force Headquarters–Cyberspace

As a part of the Cyberspace Mission Force, and as defined in the Joint Staff execution order, USCYBERCOM designated each service's cyberspace component (the Air Force example is AFCYBER) a Joint Force Headquarters–Cyberspace and directed each one to support specific combatant commands. These headquarters provide cyberspace domain expertise, enabling the supported combatant command staff to integrate the necessary operational- and tactical-level cyberspace planning activities into operational plans. Additionally, Joint Force Headquarters–Cyberspace executes OPCON to the tactical firing units known as combat mission teams and combat support teams, which are aligned to specific target sets within their respective combatant commands. The joint cyberspace center, cyberspace support element, and Joint Force Headquarters–Cyberspace establish unity of command and unity of effort for the combatant commander's (or joint force commander's, if established) cyberspace operations through direction of the attached combat mission and support teams.

Combat Mission Team / Combat Support Team

Combat mission teams concentrate on combatant commander's objectives and project power in and through cyberspace while combat support teams offer analytical and developmental support to combat mission teams. Under both C2 frameworks, to leverage the combat mission teams' capabilities, air component planners must

request cyber effects that support the JFACC's objectives. Just as there are a limited number of aircraft, so are there a limited number of combat mission teams and combat support teams. As a result, every request made by the air component may not be immediately pursued. The joint cyberspace center reviews and validates all requests by the components to ensure not only that the effect supports the respective component's objectives but also that the request is one which the combatant commander wishes to dedicate the constrained resources of his or her combat mission team and combat support team towards pursuing. Clearly, the JFACC must be certain that cyberspace planners coordinate closely with their respective joint cyberspace center.

Director of Cyberspace Forces

The current push from the Air Force entails setting up a position with a familiar name: director of cyberspace forces, working for the JFACC. There are many issues with the establishment of this position, the most notable of which is that it runs counter to the Joint Staff execution order defining coordination authority within the joint cyberspace center (direct support model) or the joint force cyberspace component commander (OPCON model) since the name implies that it has that coordination authority, as do other similar positions.

The director of cyberspace forces was originally Air Forces Central Command's solution to supporting the air and space operations center with cyberspace operations. The command modeled the director of cyberspace forces after the director of space forces and the director of mobility forces. This position was intended to give the commander, Air Force forces a senior expert for cyberspace operations. While Air Forces Central Command authored the concept in June 2014 to establish a director of cyberspace forces, the Joint Staff began standing up the Cyberspace Mission Force with the release of the previously mentioned 2013 Joint Staff Execution Order "Implementing Cyberspace Operations Command and Control."

In a joint task force, the JFACC is normally delegated space coordination authority from the joint force component commander.[2] In that instance, the director of space forces is the primary adviser to the JFACC on space operations. In a joint force, each component knows to find the director of space forces to coordinate space requirements for the joint area of operations. So although the director of space forces works for the JFACC, that individual provides "space-enabled effects to the [joint task force] based upon [joint force component] priorities."[3] Similarly, the director of mobility forces has a joint perspective and responsibilities to the joint force component for both internal and external air mobility operations. The director of mobility functions as a coordinating authority with all required commands and agencies for mobility operations. Once again, if a component in the joint force needs mobility expertise or advice, it knows to find the director of mobility forces. One other key note is that the director of space forces and the director of mobility forces are both recognized by joint publications, but the director of cyberspace forces is not.[4] JP 3-12(R), *Cyberspace Operations*, 5 February 2013, also makes no mention of the position.

The director of cyberspace forces position at the combined air operations center lacks the same coordination authorities that exist for the director of space forces and director of mobility forces. The latter two are joint-task-force-level positions and serve as lead advisers for their respective specialties. In Air Forces Central Command's situation, the director of cyberspace forces working for the combined force air component commander is not the joint-task-force-level lead for cyberspace operations; that is the role of the joint cyberspace center in the Cyberspace Mission Force construct. Additionally, the combatant command's joint cyberspace center receives direct support from the Joint Force Headquarters–Cyberspace, which in turn has OPCON over its respective combat mission teams and combat support teams.

Outside Air Forces Central Command, the director of cyberspace forces is now being championed. The question that hasn't been fully explored has to do with problems that will be solved by creating the director of cyberspace forces. What will be different or better when that director conducts his or her daily job? The position has no authorities with respect to offensive cyberspace operations missions as a part of the Cyberspace Mission Force; those authorities flow from USCYBERCOM through Joint Force Headquarters–Cyberspace to the combat mission team. Assuming that offensive cyberspace operations are the mission type that the JFACC cares most about, the director of cyberspace forces will only coordinate with the appropriate agencies to support the JFACC's requests for offensive cyberspace operations. The authorities of the director of cyberspace forces for defensive cyberspace operations and DOD information network operations are also lacking.

The identified problem that brought about this resurgent discussion of director of cyberspace forces is that the JFACC is not receiving an adequate level of support and integration from cyberspace forces. The director of cyberspace forces was identified as the answer to this problem, but the director is possibly only a small part of the solution. The true problem is larger than missing a "single face" for all things cyberspace. It is a classic organize, train, and equip issue for the air component. The Air Force must reassess where cyberspace professionals are placed in air and space operations center divisions, including cyberspace-focused intelligence professionals. The current construct, which places cyberspace professionals in a specialty team, is no longer sufficient to fully integrate cyberspace effects. To push the air component towards the ultimate goal of a multidomain operations center, planners of nonkinetic effects must be placed inside in the strategy; combat plans; combat operations; and intelligence, surveillance, and reconnaissance division. As long as the direct support model is in effect, liaisons from the joint cyberspace center and Joint Force Headquarters–Cyberspace must be brought into the air component to form the cyberspace operations coordination element, just as the Marine, Navy, and special operations forces send liaisons to integrate. Lastly, cyberspace planners in the air component lack the proper intelligence-driven planning systems. This work is still in progress and is not unique to the JFACC's operations.

Solution: The Joint Air Component Coordination Element

A proven way for the JFACC to coordinate with other component commanders' headquarters is the joint air component coordination element (JACCE). Sending a JACCE to the joint cyberspace center to support the JFACC's objectives will offer an Airman's perspective to the future cyberspace component and allow for enhanced planning, integration, and execution of offensive cyberspace operations missions. In his article "A Seat at the Table: Beyond the Air Component Coordination Element," Gen Mike Hostage, USAF, retired, advocates for not only sending a JACCE to joint force component organizations but also ensuring that his or her daily interactions, resources, and authorities are appropriate for the mission.[5] Therefore, the JFACC should ensure documentation of the JACCE's authorities that are sent to the joint cyberspace center. The JACCE will receive support from the air component's cyberspace planners within the divisions and staffs.

The idea of sending the JACCE to the joint cyberspace center (or the future cyberspace component) is the same as the air component sending JACCEs to other components. By applying a proven way to integrate air component operations, such as the JACCE, the air component will be better set up for success to integrate cyberspace operations for the JFACC while aligning organizationally and working within the constraints of the Cyberspace Mission Force. The JACCE is already charged with coordinating the integration of requirements as "airspace coordinating measures, fire support coordinating measures, close air support, air mobility, and space requirements."[6] Now cyberspace operations should be added to that list.

As previously addressed, the joint cyberspace center, in turn, should send cyberspace liaisons to the air component to integrate joint cyberspace operations. A major step in the center's maturation process is coordinating with components. A cyberspace operations liaison element sent to the air component to plan and integrate joint cyberspace effects will only help. The element will carry out functions similar to those of the special operations liaison element, battlefield coordination detachment (Army liaisons), naval and amphibious liaison element, and Marine liaison officer, which already exist as recognized liaisons within the air component. The Air Force should focus and shape its cyberspace operations efforts through the JACCE, which, with a collection of cyberspace experts from all three cyber mission areas—DOD information network operations, defensive cyberspace operations, and offensive cyberspace operations—can then ensure that the JFACC's objectives and priorities are being met.

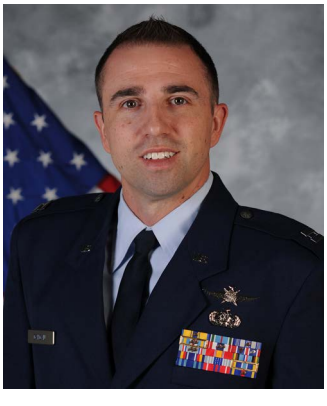
Conclusion

How can the JFACC gain access to, integrate, and C2 offensive cyberspace operations? He or she can do so by understanding the available cyberspace forces and requesting support from them, comprehending cyberspace guidance and the Joint Staff Execution Order on "Implementing Cyberspace Operations Command and Control," and setting the foundation for the JFACC to leverage offensive cyberspace operations through a JACCE to the joint cyberspace center (or cyberspace component). The JFACC can then fix manning within the air component to have cyber-

space planners in the proper divisions (and not in special teams) to link the requested targets and effects to JFACC objectives within the joint air operations plan and air operations directive, including cyberspace support from the joint cyberspace center. Finally, the JFACC can work with the joint cyberspace center and Joint Force Headquarters–Cyberspace to stand up the cyberspace operations liaison element within the air component to ensure proper understanding of the JFACC's objectives and areas where he or she can provide support. ✪

Notes

1. Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations*, 10 February 2014, I-1, http://www.dtic.mil/doctrine/new_pubs/jp3_30.pdf.
2. JP 3-14, *Space Operations*, 29 May 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.
3. Curtis E. Lemay Center for Doctrine Development and Education, "Director of Space Forces," in "Annex 3-14, Space Operations," 19 June 2012, [1], https://doctrine.af.mil/download.jsp?filename=3-14-D17-SPACE-OPS-DIRSPACEFOR.pdf.
4. JP 3-14, *Space Operations*; JP 3-30, *Command and Control of Joint Air Operations*; and JP 3-17, *Air Mobility Operations*, 30 September 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_17.pdf.
5. Lt Gen Mike Hostage, "A Seat at the Table: Beyond the Air Component Coordination Element," *Air and Space Power Journal* 24, no. 4 (Winter 2010): 18–20, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj10/win10/2010_4.pdf.
6. Curtis E. Lemay Center for Doctrine Development and Education, "The Joint Air Component Coordination Element," in "Annex 3-30, Command and Control," 7 November 2014, [1], https://doctrine.af.mil/download.jsp?filename=3-30-D29-C2-JACCE.pdf.



Capt Jason M. Gargan, USAF

Captain Gargan (BS, MS, Bellevue University) is chief of cyberspace integration and an instructor at the US Air Force Weapons School, Nellis AFB, Nevada. He is responsible for the integration of cyberspace and information operations into all weapons school exercises. The author of multiple offensive cyberspace operations courses, he instructs all students who attend the school on what cyberspace effects can bring to the battlefield. Captain Gargan recently returned from Air Forces Central Command's combined air and space operations center, where he stood up the cyberspace operations cell within the strategy division. As the first cyberspace weapons officer to deploy to Air Forces Central Command, he was responsible for a team that planned all offensive cyberspace fires in support of Operation Inherent Resolve against Da'esh terrorists. Prior to becoming a weapons school instructor, he was the chief of standardization and evaluation for the offensive cyberspace operation weapon system utilized by the Air Force's Network Attack System.