Office of Naval Research Project BlueShark creates high-tech, futuristic environment to demonstrate what operational work environments might look like and what emerging innovative technologies might provide in next decade (U.S. Navy/John F. Williams)

The Joint Force Commander's Guide to Cyberspace Operations

By Brett T. Williams

Joint force commanders (JFC) earn the right to command because, regardless of their "native" domain, they are able to direct joint operations in the land, maritime, air, and space domains to achieve campaign objectives. Commanders must develop the same capability to direct operations in the cyber domain since mission success increasingly depends on freedom of maneuver in cyberspace. The preeminent JFC requirement for freedom of maneuver in cyberspace is command and control (C2). It is impossible to fully employ today's joint force without leveraging cyberspace. Other examples include the fact that cyberspace is heavily used to support shaping and influence operations, particularly in the realm of deterrence. The ability to collect, analyze, and use intelligence information depends on cyberspace. Moving data from sensor to shooter and getting access to information all the way to the tactical edge are fundamental requirements for cyberspace. Finally, there are evolving opportunities to project power in and through cyberspace to support attaining campaign objectives. Since cyberspace operations

Major General Brett T. Williams, USAF, is the Director of Operations, J3, for U.S. Cyber Command.

are fundamental to success, commanders cannot continue to run the risk of inappropriately delegating key operational decisions because they and their staffs lack an understanding of the domain. This article argues that despite the technical complexity of cyberspace, the JFC can and should direct cyberspace operations at the operational level of war using current operational doctrine and existing planning and execution processes.

Some people are reluctant to read about cyberspace because they perceive the subject to be "too technical." This piece is intentionally written in the lexicon of joint operations to make it easily understandable, but more importantly to make the point that at the operational level, we must plan and execute cyberspace operations just as we do land, maritime, air, and space operations. What prevents us from taking this approach today is a lack of shared cyberspace knowledge and an agreed upon operational approach that links cyberspace missions and actions and places them in the larger context of joint operations.

The approach outlined here contributes to a shared understanding of cyberspace that is necessary for senior decisionmakers both inside and outside the Department of Defense (DOD). When senior leaders meet to shape national security policy, consider operational plans, or allocate resources, common shared experience means that decisions related to the land, maritime, air, or space domain rarely require accompanying background information regarding the roles and functions of units or weapons systems. The same is not true for cyberspace operations, yet we attempt to structure the meeting in the same way: "Skip the background and get to the decision slide." The risk in this approach is de facto decisionmaking by the people who prepared the brief. There is too much at stake for our senior leaders not to understand cyberspace operations in the same way they understand operations in the other domains. The approach to cyberspace articulated here is useful because it is understandable without a degree in computer science, significant expertise in signals intelligence, or the ability to configure a firewall. At the same time, it is unrealistic to think that we are going to conduct operations in cyberspace without learning some new concepts and associated terminology, at least to the level of this article.

This operational approach will be effective only if we take the time to evolve current conflict theory to account for cyberspace. There is an analogy with airpower here. Airpower did not change the nature of war, but it did change its character. We had to alter our mental framework for conflict to account for the unique capabilities of airpower. In the same way we had to develop airpower theory and make adjustments to broader conflict theory, we need a theory for cyberspace operations that will allow us to understand the implications of employing cyberspace capabilities at the tactical, operational, and strategic levels. The theory must capture the ubiquitous nature of cyberspace and its relevance and interaction with government, commercial, and civilian sectors. Additionally, the theory must cover the complete spectrum from national security policy to detailed technical operations and account for the fact that the domain changes constantly. The process of operational design could be useful in this endeavor.

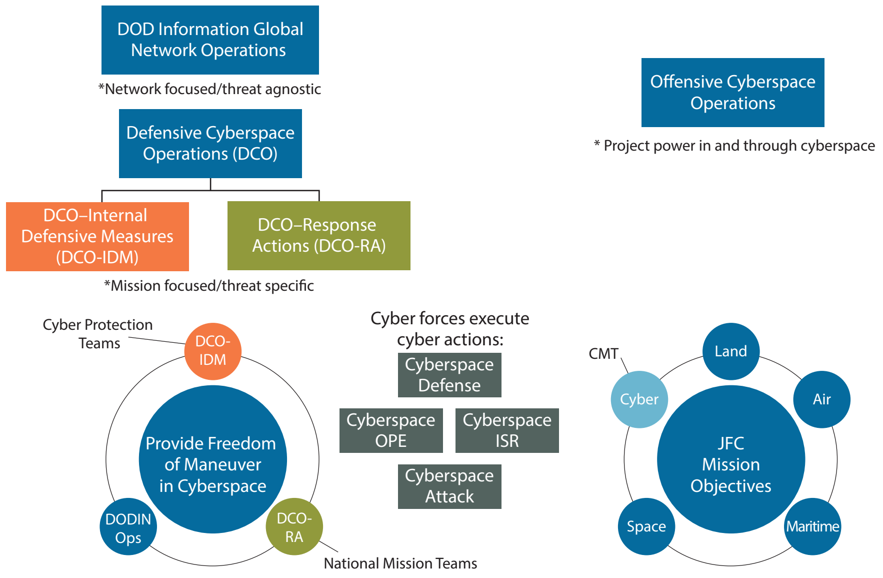
This approach to cyberspace operations reflects the work of the author and his colleagues that began at U.S. Pacific Command and substantially evolved at U.S. Cyber Command (USCYBERCOM). As much as possible, we use the terminology and processes found in the following joint publications (JPs): JP 1, *Doctrine for the Armed Forces of the United States*, JP 3.0, *Joint Operations*, JP 5.0, *Joint Operation Planning*, JP 3.12, *Cyberspace Operations*, and JP 3.60, *Joint Targeting*. The first section presents four axioms developed by the author that underpin the main thesis that we can and should approach cyberspace operations just as we approach operations in the other domains. The next two sections describe an operational approach that allows a JFC to provide friendly freedom of maneuver in cyberspace and to project power in and through cyberspace in support of campaign objectives. The final section describes individual cyberspace actions that create the effects to execute the operational approach. Although this article focuses on DOD operations, the concepts are applicable to any organization that finds itself at risk from malicious cyberspace activity.

Four Axioms

Axiom #1. Use of the term *cyberwar* is not productive. War, conflict, and competition are all characterized by enduring principles that were established long before cyberspace. The creation of cyberspace has simply offered another environment or domain within which to exercise the elements of national power. Focusing inordinately on the unique nature of cyberspace operations at the tactical level tends to draw senior policymakers and their military commanders into a narrowly defined view of conflict and away from a whole-of-government approach to both policy and operations. The result is a tendency to overstate the relevance of cyberspace operations within the context of all other activities that influence the actions of people with opposing goals. Relying on tactical actions from any single domain to be "dominant" is a pitfall that we have mostly learned to avoid, and we should not have to relearn the lesson as we integrate cyberspace operations into joint planning. It is the integration of land, maritime, air, space, and cyberspace *operations* that achieves *campaign* objectives.

Axiom #2. Established joint doctrine accommodates operations in cyberspace quite well, so we do not need to invent anything new. USCYBERCOM staff has found that there are few adjustments required to integrate cyberspace operations into existing planning and execution processes. The joint operation planning process (JOPP) that uses mission analysis to produce a plan or order adapts well to cyberspace operations. In a similar way, the joint targeting cycle, which begins with an endstate and commander's objectives and continues with target development, weaponeering, execution,

Figure 1. Cyberspace Operations


DOD Information Global Network Operations
*Network focused/threat agnostic
Defensive Cyberspace Operations (DCO)
DCO–Internal Defensive Measures (DCO-IDM)
DCO–Response Actions (DCO-RA)
*Mission focused/threat specific
Offensive Cyberspace Operations
* Project power in and through cyberspace
Cyber Protection Teams
DCO-IDM
Provide Freedom of Maneuver in Cyberspace
DODIN Ops
DCO-RA
National Mission Teams
Cyber forces execute cyber actions:
Cyberspace Defense
Cyberspace OPE
Cyberspace ISR
Cyberspace Attack
CMT
Land
Cyber
Air
JFC Mission Objectives
Space
Maritime

Supported by all-source intelligence, information technology, and routine communications activities

and assessment, readily accommodates cyberspace targeting.

Axiom #3. We have a pressing need to develop cyberspace operators who are credible and effective in the J3 (operations) and J5 (strategic plans and policy) within both the Joint Staff and combatant commands. For emphasis, that is the J3 and J5, not just the J2 (intelligence) and J6 (command, control, communications, and computers systems), and at all of the combatant commands, not only USCYBERCOM. Despite the technically complex nature of cyberspace and the potential for increasing levels of machine-to-machine interaction, success will always rely on the leadership and technical skills of Soldiers, Marines, Sailors, and Airmen. Joint staffs consist of what we typically think of as operators, members of the combat arms who are educated, trained, and experienced in operations. Cyberspace expertise usually comes from people with intelligence, communications, or cryptology backgrounds—career fields typically categorized as support forces. If we are going to treat operations in cyberspace like operations in the other domains, the Services must commit to unique career fields for cyberspace. There has been a focus on providing highly trained, technically skilled personnel who come mostly from the enlisted or warrant officer ranks. DOD must rapidly bring the same emphasis to cyberspace officer career development. Cyberspace, like the other domains, requires officers who are developed across their careers in a way that positions them to lead at senior levels in both command and staff. Cyberspace officers should spend their first 10 years becoming tactically proficient in all aspects of cyberspace operations, complete Service and joint military education, serve on joint staffs, command in their areas of operational specialties, and do all the other things necessary to produce general and flag officers whose native domain is cyberspace.

Axiom #4. Words matter. Routine misuse of the word *cyber* is one reason we do not have a common framework for discussing cyberspace operations. *Cyber* is neither a verb nor a noun that can stand on its own. Saying "cyber" should not automatically connote offensive operations. Additionally, questions such as "Is cyber intel?" or "Is cyber comm?" are counterproductive as they encourage legacy stovepiped views of cyberspace operations. *Cyber* is most useful as part of the compound word *cyberspace*, and cyberspace is simply the manmade domain and information environment we create when we connect together all computers, wires, switches, routers, wireless devices, satellites, and other components that allow us to move large amounts of data at very fast speeds. It follows that cyberspace operations are those conducted in cyberspace with the objective of providing friendly freedom of maneuver in cyberspace and projecting power in and through the domain in support of JFC campaign objectives. Intelligence and communications are support functions to cyberspace operations just like intelligence and communications support operations in all the other domains. Both intelligence and communications functions must be more closely integrated with cyberspace operations than operations in the physical domains; however, it is important to maintain the distinction between supporting activities and the operations themselves.

Missions and Objectives

Building on these four axioms, we can now describe cyberspace operations in terms of intent, mission categories, and actions. In anticipation of at least a few fighter pilots and infantry officers reading this, it has been necessary to include a picture that will serve as a reference for the discussion. The test at the end is being able to define the terms and articulate the interrelationships depicted in figure 1 to indicate the minimal level of understanding necessary for commanders and their staffs to plan and execute cyberspace operations.

The two cyberspace objectives relevant to the JFC are providing freedom of maneuver in cyberspace and projecting power in and through cyberspace to achieve campaign objectives. There are three categories of cyberspace missions for attaining these two objectives:

- DOD information network operations (DODIN Ops)
- defensive cyberspace operations (DCO)
- offensive cyberspace operations (OCO).

Cyberspace forces execute four actions to create the necessary effects in the domain:

- cyberspace defense

- cyberspace operational preparation of the environment (OPE)
- cyberspace intelligence, surveillance, and reconnaissance (ISR)
- cyberspace attack.

DODIN Ops Mission

Providing freedom of maneuver in cyberspace must be the JFC's top cyberspace priority because of the reliance on cyberspace for command and control across the joint force. Effective C2 allows the commander to get information, move information, and use information to make better decisions faster than the enemy, which is an advantage we cannot give up and cannot achieve without assured access to cyberspace. It must be acknowledged that cyberspace will always be a contested domain, and it is unlikely we will ever have continuous or uncontested cyberspace superiority; however, in the same way we approach operations in the other domains, we must have sufficient control of cyberspace at the time and place we need it. We provide the requisite level of freedom of maneuver in cyberspace through the mission categories of DODIN Ops and DCO.

DODIN Ops include designing, building, configuring, securing, operating, maintaining, and sustaining the information environment that we rely on for operations. DODIN Ops should be done in a proactive manner and include actions focused on information technology (IT) consisting of hardware and software, data, individual users, and system administrators. Examples include correcting known IT vulnerabilities, encrypting data, and ensuring user and administrator training and compliance. It is useful to think of DODIN Ops as being "network" focused and threat agnostic. They are *network focused* in that they approach security from the perspective of IT in the operational configuration. Traditionally, DODIN Ops have not emphasized the security of data at rest or in motion within or across the information environment, even though it is the integrity and security of the data that matter most to the commander. They are *threat agnostic* in that their security measures are not focused on a specific threat. Instead, our security baseline seeks to mitigate known vulnerabilities from a broad range of threats. For the same reason people lock their car doors regardless of where they park or the fact that we check identification at the gate, it is prudent to establish a level of security to defend our information environment against a general category of malicious cyberspace activity to include insider threats. A useful byproduct of establishing strong baseline security is that it makes the cyberspace terrain a hard target and encourages adversaries to go after softer ones.

A key tenet of DODIN Ops is to provide a consistent level of security across all components of the DODIN. This is important for three reasons. First, the nature of cyberspace, as currently architected, means that a risk shared by one is a risk shared by all. Just as a single negligent sentry puts an entire base at risk, a single careless user or system administrator introduces risk to an otherwise secure network. Second, the majority of malicious activity in the DODIN can be mitigated with currently available techniques since the vast majority of adversary exploitation utilizes known vulnerabilities. The vulnerabilities are not corrected for a variety of reasons to include lack of resources (time, people, money), inadequate leadership emphasis, hubris ("We are really good, no one can get into our network"), or simple ignorance of the security requirements. Third, strong security compliance allows us to focus our efforts on the most sophisticated threats. All too often our most capable people spend the majority of their time dealing with serious compromises that could have been prevented with basic security compliance.

Even perfectly executed, the security provided through DODIN Ops is not sufficient alone to defend our information environment. Until we substantially evolve the architecture, a variety of technical and policy challenges will continue to inhibit our ability to evaluate, report, and correct compliance deficiencies. Efforts are under way to address these technical challenges specifically with DOD's Joint Information Environment (JIE). Making JIE a reality soon is critical to providing defensible cyberspace, but no matter how much we improve technically, leadership awareness and command accountability will remain essential to cyberspace security. Commanders need to treat the DODIN like the weapon system it is and hold both users and network operations personnel accountable for their actions. The constantly changing nature of the domain, the low price of entry for malicious actors, and the large potential payoff for cybercriminals, hacktivists, or nation-states means that we must do more than make passwords 15 characters long. Commanders must prioritize resources to achieve the highest possible compliance with IT security directives. Doing so sets the first line of defense in a layered cyberspace defense strategy. Unfortunately, even perfect DODIN Ops execution is not sufficient to provide freedom of maneuver in cyberspace. Defensive cyberspace operations are required to engage and defeat the full range of cyberspace threats.

DCO Mission

Defensive cyberspace operations are passive and active cyberspace defense activities that allow us to outmaneuver an adversary. The ultimate goal of DCO is to change the current paradigm where the attacker enjoys significant advantage. DCO provide the ability to discover, detect, analyze, and mitigate threats, to include insider threats. As opposed to DODIN Ops, we should think of DCO as mission focused and threat specific. They are *mission focused* because they are prioritized against key cyber terrain to ensure data move securely across the information environment. They are *threat specific* because they are executed against specific threats with malicious capability and intent to affect our key cyber terrain. The first step in directing the DCO mission is having the commander identify the key cyber terrain. For example, if missile defense is a priority then perhaps the Ballistic Missile Defense System (BMDS) is key cyber terrain. Step two in this example is technically enumerating the key cyber terrain from sensor to shooter. Essential elements of the key cyber terrain for BMDS include the various sensors that collect launch data and the networks and systems that move that data to a variety of command centers for attack assessment. From there, the data must move quickly and securely to direct an appropriate response. One rapidly determines there are many systems involved, all with their own vulnerabilities along with additional vulnerabilities at the points where one system connects to another. There are more vulnerabilities than we can address, and therefore we must prioritize our efforts against adversaries with specific capability and intent to interfere with our key cyber terrain.

By linking vulnerabilities with adversary capability and intent, we have identified the primary risk areas on which to focus our defensive efforts. Defending BMDS or any other key cyber terrain involves both subcategories of DCO: internal defensive measures (IDM) and response action (RA). IDM are those actions we take internally to friendly cyberspace, and RA is taken outside our information environment to stop or block the attack.

The essential tasks for DCO-IDM are hunting on friendly cyber terrain for threats that evade our security and directing appropriate internal responses. There are several key requirements for effective DCO-IDM. First, there must be sufficient personnel specifically trained to operate on the individual systems and components that make up the key cyber terrain. Second, we must have timely intelligence and information-sharing as well as shared situational awareness to direct the actions of the hunt mission; simply wandering the network looking for things that do not "look right" is not going to work. Third, we have to evolve how we think about authorities to operate on friendly cyberspace. In any example of key cyber terrain, there will be multiple network authorities and program managers. Ultimately, the appropriate commander must have the authority to direct DCO forces to operate across the entirety of the key cyber terrain. Finally, we must create capacity and diversity in DCO-IDM forces. Most of the current capability exists at the global level, and there are a variety of technical and policy limitations that degrade effectiveness. Effective DCO-IDM requires forces that can operate at all levels in the DODIN in a coordinated fashion. USCYBERCOM has defined the need for Cyber Protection Teams (CPT) to conduct the DCO-IDM mission. CPTs are training to a high technical standard, and their capabilities include analyzing key cyber terrain, hunting on friendly cyber terrain, and emulating threats to test defenses.

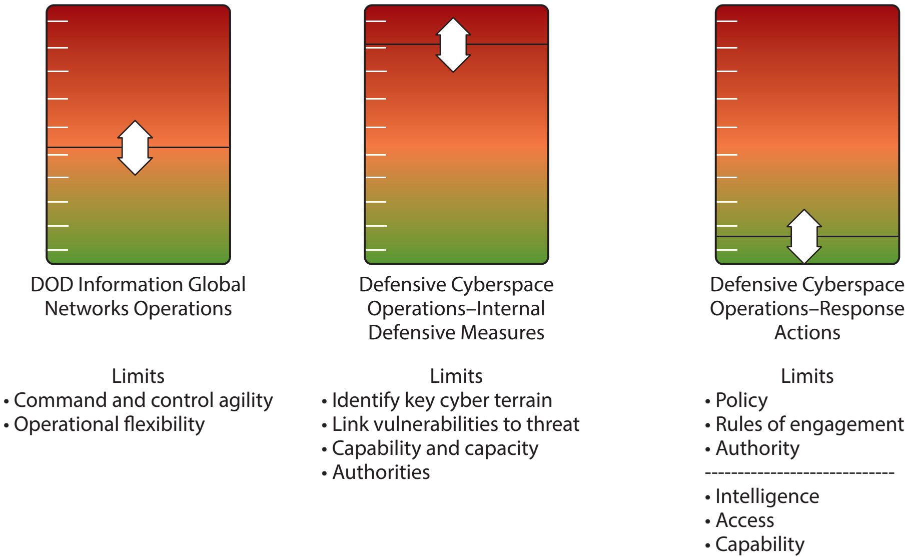
The essential task for DCO-RA is to "kill the archer." We catch arrows with DODIN Ops and DCO-IDM. DCO-RA, however, is about going after the shooter. We do not defend an airfield solely with hardened shelters, surface-to-air missiles, and fighters overhead. By analogy, we should not expect to defend our information environment with DODIN Ops and DCO-IDM alone. In the same way we go into enemy airspace to shoot down airplanes, crater a runway, or destroy a C2 facility, the commander needs options to conduct DCO-RA outside friendly network space to stop the attack before it reaches our key cyber terrain. The forces tasked with the DCO-RA mission under the USCYBERCOM model are the National Mission Teams (NMTs), which are trained to the highest technical standards. They operate in accordance with all the legal and policy guidance impacting operations outside friendly cyberspace. NMT success relies on timely intelligence, information-sharing, shared situational awareness, and close synchronization with the CPTs executing the DCO-IDM mission.

The JFC Integrated Approach

As with any military operation, actions along a single line of effort rarely accomplish the commander's scheme of maneuver, and the same holds true in cyberspace. To provide freedom of maneuver in cyberspace, we must optimize the employment of forces across DODIN Ops, DCO-IDM, and DCO-RA. One way to think about this employment construct is to envision a lever that controls each of the three mission areas. There are constraints, restraints, costs, benefits, and risks associated with moving the levers up or down, and there are impacts across all three mission areas when any single lever is moved. Commanders must achieve a balance that satisfies their mission objectives at an acceptable level of risk. Figure 2 is a visual depiction of this concept.

The lever on the left represents DODIN Ops and is set at the baseline

Figure 2. Providing Freedom of Maneuver in Cyberspace


DOD Information Global Networks Operations
Limits
• Command and control agility
• Operational flexibility
Defensive Cyberspace Operations–Internal Defensive Measures
Limits
• Identify key cyber terrain
• Link vulnerabilities to threat
• Capability and capacity
• Authorities
Defensive Cyberspace Operations–Response Actions
Limits
• Policy
• Rules of engagement
• Authority
• Intelligence
• Access
• Capability

security level. Moving the lever up "hardens" the environment through actions such as restricting access to and from the DODIN, isolating high-risk applications or services, and rerouting traffic to enable more effective sensor coverage. We should carefully consider moving this lever up since network hardening tends to reduce C2 agility and operational flexibility.

The center lever represents DCO-IDM and is the linchpin to providing freedom of maneuver in cyberspace. Hunt operations and key cyber terrain analysis enable both the DODIN Ops and DCO-RA missions as long as there is effective information-sharing and maneuver synchronization. We would like to push the DCO-IDM lever all the way up, but there are significant limits. For instance, it could be challenging just to get the commander's staff to identify key C2 requirements by operational phase. As described above, the process of technically enumerating the key cyber terrain and its associated vulnerabilities is a large technical challenge. Correlating enemy capability and intent with known vulnerabilities is another level of complexity. Manning, training, and equipping sufficient teams is a major hurdle. Finally, there are myriad authorities' issues involved when working across multiple networks, systems, applications, and services.

The third lever is DCO-RA, which we would also like to push all the way to the top, but we have to account for two categories of limitations that are exactly analogous to operating in the physical domains outside of friendly space. The first limits are the constraints of policy, rules of engagement (ROEs), and authority for execution. We are challenged by the fact that these constraints are constantly evolving as both the domain and our understanding of the domain change. Adding to this challenge, many of our senior leaders have a limited understanding of cyberspace operations, and that lack of understanding can lead to risk aversion or unhelpful focus on tactical issues. The second set of limits describes the same restraints associated with any target. The planner has to have the intelligence support to understand how the target system operates, access to the target, and the capability to impact the target to generate the desired effect. Cyberspace targeting is complicated by the rapidly changing nature of the target systems, the extensive target development required to achieve a weaponized solution, and our nascent ability to describe both desirable and undesirable effects for cyberspace operations. Integrating cyberspace targeting within the existing construct of joint targeting and the creation of a Joint Munitions Effectiveness Manual for cyberspace capabilities are major steps in the right direction.

Here is a simple example of how this operational approach provides a response to a malicious cyber event. Assume we have intelligence indicators that an adversary is going to launch a cyber attack against a key C2 system, and we have identified 100 compromised servers around the world that will host malware for the attack. Working from left to right across our levers, we would determine if moving the DODIN Ops lever would allow hardening actions that would reduce our attack surface with acceptable operational impact. We would then task our DCO-IDM forces to focus on the highest risks on the key cyber terrain. It is unlikely that we would have sufficient forces to cover all the key cyber terrain, so we would request additional support through the normal Request for Forces process. Next we would examine DCO-RA options to determine if there are any preauthorized, preplanned actions that could be taken to block the attack. We would have to first verify that planned actions had not been rendered ineffective due to changes in the targeted networks. Then we would need to confirm that existing ROEs and authorities were sufficient for the commander to order execution. If not, the commander could request the necessary additional authority to engage the enemy. If the ROEs were not expanded, we would potentially have to harden the network and/or redirect DCO-IDM capability and accept risk in other portions of the key cyber terrain. It is important to note that even without authorization to stop or block the attack, the DCO-RA mission is critical for intelligence purposes. The DCO-RA forces operating in adversary space provide critical information regarding attribution; adversary tactics, techniques, and procedures; and exposing capabilities not yet deployed. Such intelligence information is critical for executing DODIN Ops and DCO-IDM. Our BMDS defense example shows that providing freedom of maneuver in cyberspace requires a coordinated, synchronized, integrated planning and execution process across all three missions. Key to success is that all forces are trained to the same high standard and that they have access to the same intelligence. We cannot treat DODIN Ops and DCO-IDM as maintenance activities with no need for highly skilled personnel or sensitive intelligence information.

Cyberspace Integration

Turning now to the right side of figure 1, we can discuss integration of cyberspace operations with operations in the physical domains to achieve JFC campaign objectives. The best way to integrate cyberspace operations is to use the commander's existing JOPP. Experience at USCYBERCOM suggests that standard doctrinal planning and execution processes work for cyberspace operations. Existing boards, bureaus, cells, and working groups that do mission analysis, course of action development, center of gravity determination, collection management, targeting (both deliberate and dynamic), and assessment all require little if any adaptation to account for cyberspace operations. Of course, personnel with appropriate cyberspace operations experience must be integrated into the commander's joint staff in the same way the staff has the requisite mix of officers with land, maritime, air, and space experience. Additionally, trained and ready cyberspace forces must be made available, and there must be an effective C2 structure with associated processes supported by the right information environment and effective knowledge management tools.

A complete C2 discussion is beyond the scope of this article, but a key element

Sailors conduct duties at U.S. Fleet Cyber Command Maritime Operations Center, Fort Meade, Maryland (DOD)

for success is the designation of a joint force cyberspace component commander (JFCCC) who operates at the same operational planning and execution level as the functional component commanders for the land, maritime, and air domains. The JFCCC will direct DODIN Ops and DCO to provide freedom of maneuver in cyberspace and will direct offensive cyberspace operations (OCO) to project power in and through cyberspace. The JFCCC will work with the other component commanders to establish supported and supporting roles throughout all phases of the operation. Those familiar with OCO in the context of recent conflicts may infer that the greatest utility lies in Phase 0 and I to support shaping operations, information operations, military deception, and preparation of the environment. OCO will continue to play a key role in these early phases; however, in future engagements these operations will increasingly provide opportunity for significant impact throughout the campaign. Worth noting is that the JFCCC and associated cyberspace forces operate during both steady state and crisis similar to a theater special operations command and that the USCYBERCOM commander has combatant command responsibility for those forces (similar to U.S. Special Operations Command) in order to globally synchronize and integrate activities in cyberspace.

This description is not meant to oversimplify the process of integrating cyberspace operations into JFC planning and execution, and admittedly there are three major challenges that make this difficult. First and foremost, the JFC does not have access to cyberspace operators—officers who are trained from commissioning at the tactical level in all three mission areas—DODIN Ops, DCO, and OCO—and then professionally developed as joint warfighters. Until we develop such officers, we will continue to rely on members of the traditional combat arms to learn enough about cyberspace to integrate cyberspace operations into the planning and execution process they already understand. The second challenge is the level of security we have attached to many cyberspace operations. High levels of security compartmentalization can inhibit integrated planning and execution, and this dynamic is not unique to cyberspace. The third challenge is authorities. One could argue that it is more likely to receive an execute order authorizing kinetic action that could result in death and destruction than it is to expect a JFC to be delegated authority to conduct DCO-RA or OCO. Hesitancy to delegate authority for cyberspace operations is a reflection of our limited shared understanding of cyberspace and in some cases erroneous preconceived notions about the domain. For actions in the physical domains, we are comfortable with issues of sovereignty, probability of kill, anticipated collateral damage, and fratricide. Because we cannot articulate these same considerations for cyberspace in nontechnical, easily understood terms, the authority for execution is typically held at a level above the JFC. One way to address this challenge is to use the standard target validation and vetting process for cyberspace targets. This would force us to address all of the normal targeting issues to include intelligence gain/loss, operations gain/loss, and, unique to cyberspace operations, technical gain/loss where we have to evaluate the risk of exposing a particular capability because that exposure may put an unrelated operation in jeopardy. Once we develop the same disciplined planning approach and precision attack capabilities for conducting DCO-RA and OCO that we have developed for prosecuting targets in the physical domains, the JFC will get execution authority.

To sum up the bottom right side of figure 1, cyberspace operations at the operational level of war can and should be treated like operations in the other domains. We do not need to invent new planning and execution processes; we just need to conduct cyberspace operations with the same disciplined approach as all other joint operations and provide commanders with the relevant considerations in familiar, understandable terms.

Cyberspace Actions

To frame the employment of forces in the cyber domain, we finish with a description of the four actions listed in the center of figure 1: cyberspace defense, cyberspace ISR, cyberspace OPE, and cyberspace attack. These actions are conducted by the JFC to execute DODIN Ops, DCO, and OCO missions. It is important not to conflate the missions with the actions. In other words, the action of cyberspace defense is not associated only with providing freedom of maneuver in cyberspace, and cyberspace attack is not conducted only for offensive purposes.

Cyberspace defense actions are conducted by the commander with authority over the information environment to protect, detect, characterize, counter, and mitigate threats and vulnerabilities. Cyberspace ISR is normally authorized under military authorities and conducted to provide critical operational information to support follow-on actions. Cyberspace OPE consists of nonintelligence actions that set the stage for follow-on operations. Finally, cyberspace attack counters the adversary's ability to achieve objectives through degradation, disruption, or destruction of infrastructure and/or capabilities. Cyberspace attack can also manipulate data in a way that impacts the adversary's information systems. It is important to recognize that cyberspace attack, like all forms of attack, is designed to generate effects in the physical domains. The desired effect may be as simple as creating uncertainty in the opponent's decision calculus, or we may seek a destructive effect that in the past could only have been possible with kinetic action. Understanding these actions and their relationships to the missions of DODIN Ops, DCO, and OCO is foundational to understanding cyberspace operations. In the same way that JFCs understands how offensive counterair contributes to air superiority and antisubmarine warfare contributes to maritime superiority, they must understand how cyberspace defense, ISR, OPE, and attack contribute to providing friendly freedom of maneuver in cyberspace.

Final Thoughts

The intent of this article is not to oversimplify or dismiss the complexity of operating in cyberspace. Instead it is to advocate for making cyberspace operations part of the powerful synergy we currently create with joint force operations. Cyberspace is difficult to visualize. We cannot create a two-dimensional Big Ass Map that we can all sit around to discuss operations. At the same time, there is a huge, largely unacknowledged benefit in that we can use existing concepts and language as a starting point to explain and teach cyberspace operations. This article is focused on cyberspace operations in support of the commander, but there is a broader implication as well. We have a requirement to determine how cyberspace impacts national security policy, grand strategy, and conflict theory; force development including personnel recruiting, development, and retention; all aspects of resourcing from joint capabilities development to programming, budgeting, execution, and defense acquisition; military support to entities outside of DOD; and force structure across the Active and Reserve components. In these and other endeavors, we should fight the temptation to invent new and unique ways of doing business. Instead we should start with the existing processes and make appropriate adjustments to account for the unique nature of cyberspace. Rarely should cyberspace operations require senior leaders to adopt a completely new frame of reference regardless of the decision at hand.

The military departments play a key role in defending our national security interests, and when the military is called into action, we rely on commanders to lead our forces. Today's commanders must be prepared to defend the Nation in all domains including cyberspace. They cannot do so without trained and ready forces, situational awareness of cyberspace, effective command and control, defensible architecture, appropriate delegation of authority for execution, and an operational approach to tie it all together. The operational approach described here provides a starting point for commanders to integrate cyberspace operations within the joint doctrinal framework employed every day to accomplish their assigned missions. JFQ