An Information Warfare Framework for the Department of Defense

Maj Andrew Caulk, USAF

Introduction

As we begin to grapple with the role the Air Force should play in the information domain, we must also lift our gaze beyond the tasks of our service to also consider the framework, or lack thereof, in which we participate.

The information environment (IE) is a noisy, risky, and asymmetric place. It is noisy in the sense that it takes a significant signal to break through the noise to create an impact. It is risky, as unlike conventional munitions, the munitions we fire here (ideas, messages, and engagements) can always be turned back against us. It is also inherently asymmetric as large actors, such as the US, present more target area to potential adversaries and often respond more slowly than smaller opponents.

P. W. Singer, author of *LikeWar*, recently said that the US has no information strategy.[1] The last time the US had something approaching a strategy was 2007.[2] This lapse is a significant shortfall. While the Department of Defense (DOD) has begun to outline information engagement concepts such as the Joint Concept for Operating in the IE (JCOIE),[3] we have yet to establish clear national or military information objectives, determine required resources to achieve those objectives, understand how to assess those objectives, or build a framework that can operationalize said objectives.

This article attempts to outline a conceptual framework that provides one potential vision to operationalize DOD information engagement. This concept is not the only way to organize. It does, however, provide a reasoned and comprehensive approach to unifying information related capabilities (IRC) across services, combatant commands (CCMD), and the DOD.

First, though, it is necessary to define the problem. Setting aside the larger, political issue of the lack of US information strategy, the overarching question for the DOD is, "What issues must the DOD address to present an effective information war-fighting capability?"

Through past observation, research, and conversations with multiple experts across IRCs, five major shortfalls emerge:

- Operational and campaigning framework
- Continuing education for IRC personnel
- Culture change through commander education
- Interagency integration
- Influence assessment and visualization

This article addresses the first shortfall while providing brief recommendations for the other four.

DOD Information Warfare Framework

There exist myriad organizations, capabilities, and authorities related to information warfare, and it seems each of those is attempting to find ways to create effects in the IE. Yet, these dispersed capabilities have no comprehensive framework that allow them to unify their efforts in a way that provides sufficient signal to noise ratio and effective engagement. Figure 1 illustrates how global reach-back capabilities could integrate through the Joint Staff and geographic CCMD commander (GCC) operational authorities to create synchronized effects.

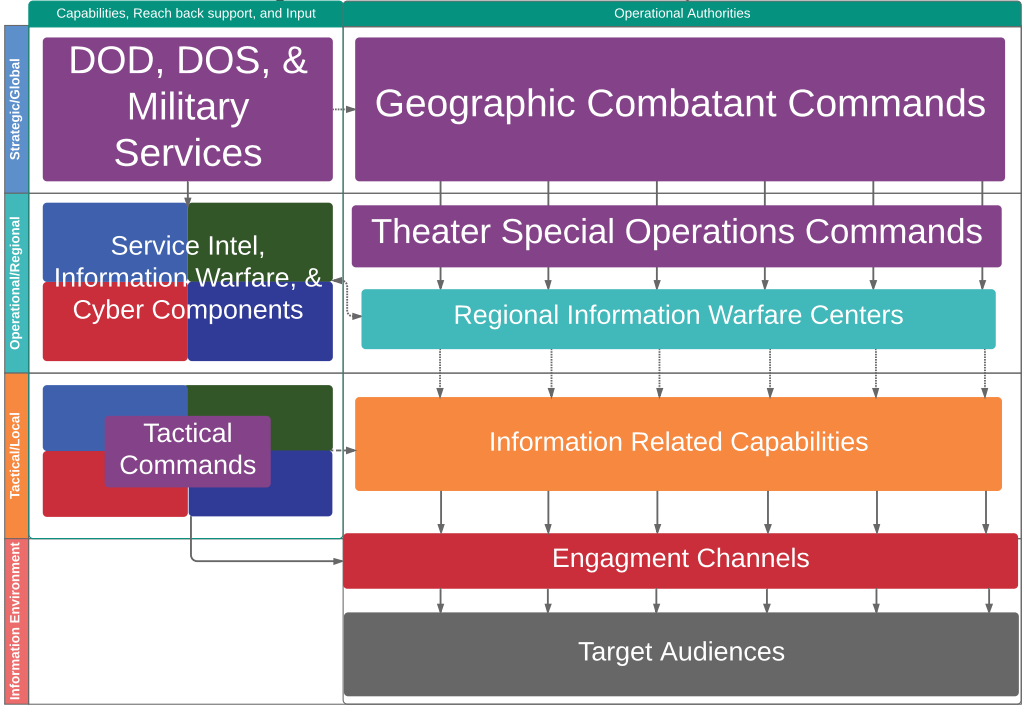

Figure 1. A concept diagram of the relationships between supported and supporting commands across the DOD

Strategic/Global Level and Authority Delegation

At the top of the figure in the blue "Strategic/Global" row sit the DOD, Department of State (DOS), combatant commands, and services. In the left column, and in the context of DOD information engagement, sit service capabilities, functional CCMDs, and the DOS are reach-back capabilities available to the GCCs. In the right column, the GCCs wield most of the operational authorities to execute information engagement, while the Joint Staff retains only the most sensitive.

Currently, IRCs' personnel, resources, and engagement authorities are fragmented across multiple GCC components and reach-back capabilities. Instead, I propose identifying one component under GCC to be the supported command for information (though other components retain their IRCs). Clearly delegating supported command status for information would be a significant shift in DOD policy as information engagement authorities are typically withheld at the GCC level or higher—presumably to mitigate perceived risk. However, such delegation would be in line with command doctrine and the idea of centralized command but decentralized execution.

Delegation is critical, and withholding engagement authorities at too high a level is ineffective for multiple reasons.

1. By design, GCC staffs will never have enough capacity to create sustained effects in the IE against all target audiences considering the required signal-to-noise ratio. A GCC's primary organizational mission is to translate national guidance into theater strategy and acquire the resources to implement that strategy. A GCC's staff, but especially the commander, simply do not have the capacity to make all decisions required by current authorities related to the IE let alone all traditional military activity. Instead, we should take direction from Joint Publication 3.0, *Joint Operations*, "Drive synergy to the lowest echelon at which it can be managed effectively."[4]

   An example that illustrates GCC staff capacity shortfalls is the comparison of lethal versus non-lethal delegation of engagement authorities. Lethal authorities are delegated to individual combat troops or units under established rules of engagement. Centralized lethal engagement authority at the GCCs level would render combat capabilities nearly ineffective—even in conflicts as small as Iraq and Afghanistan. The same holds true for nonlethal authorities in the IE as worldwide information competition is orders of magnitude larger and more complex and therefore requires further delegation.

2. Reserving authorities at such a high level distances responsible commanders from tactical input, over-aggregates information without enough

detail to adequately target, and eliminates layers of bureaucratic protection or plausible deniability from the responsible GCC. Said another way, the GCC could provide cover for an operational commander and walk back information engagement that inevitably goes astray regardless the authority level.

3. By doctrine, operational commands are designed to translate strategic guidance from GCCs into operational campaigns and orders for subordinate units.[5] Operational commands, then, are the appropriate level to "fight" in the IE as they are for conventional conflict.

4. Maintaining authorities at the GCC level creates stovepipes where any request for reach-back support must travel through a GCC's staff, then often to OSD or CJCS, then back through to service or interagency capabilities. Information engagement processes must be agile to be effective. Stove-piped coordination processes directly impede agile engagement.

This concept of delegation would require risk assumption by the GCC and for that person to trust (but verify) their subordinate commanders and campaigns. While leaders may say they trust their commanders, current bureaucratic processes communicate otherwise. If left unchecked, the over-centralization of authorities will stifle effective information engagement. Therefore, we must have critical conversations about trust and delegation moving forward.

There are many other pros and cons to delegating authority and supported command status, and opinions on the matter will differ. More debate regarding delegation is both necessary and inevitable but would be better suited for future discussion. Regardless, delegating authorities to an operational component commander, with appropriate safeguards, would seem to dramatically increase unity of command and operationalization of information for a GCC.

Operational/Regional Coordination

As depicted in figure 1, establishing connectivity at the operational level across geographic CCMDs, reach-back capabilities, and interagency organizations cuts through bureaucratic stovepipes to create an operational coordinating level that can synchronize with other GCCs and reach back to diverse US-based capabilities. Operational commands would, of course, routinely brief, synchronize, and receive input from GCCs, as each command echelon also serves in an operator role in engaging the IE.

As previously stated, Theater Special Operation Commands (TSOC) appear to be the ideal component to designate as the supported command for information for the following reasons.

1. As commands that report to both the GCC and Special Operations Command (SOCOM), TSOC can access more resources and authorities than service components. Specifically, SOCOM owns the civil affairs, counterterrorism, counterinsurgency, military information support to operations (MISO), Joint MISO WebOPS Center, and unconventional warfare capabilities.[6] TSOCs wield many of those SOCOM-specific capabilities, using both GCC and SOCOM authorities.

2. The preponderance of personnel related to direct tactical and operational information engagement (e.g., civil affairs, psychological operations, military information support teams, etc.) are assigned to TSOCs in each theater. Other components usually have only a handful of personnel in these direct engagement roles. TSOCs also tend to have much more robust J39 divisions (information operations) and supporting regional information support teams to augment information engagement planning.

3. While other components' capabilities focus on conventional warfare, TSOC forces, operating structure, and culture are tailor-made for irregular and unconventional warfare. In that vein, TSOCs often maintain a network of special operations forces liaison elements, civil military support elements, and military information support teams at specific US embassies that facilitate better region-wide coordination.

Under each TSOC in figure 1 falls an information warfare center (IWC). Only some TSOCs and GCCs have these constructs currently, and none of the TSOCs have the supported information command designation to the authors knowledge. The IWC basic concept bears a striking resemblance to an air operations center (AOC). Each would have a research, future operations, and current operations section supported by planners from each IRC as shown in figure 2. These functions mirror the strategic research, plans, and current operations divisions of an AOC. The IWC would be responsible for planning, coordinating, prioritizing, and deconflicting all component and reach-back engagement in their respective geographic theater.

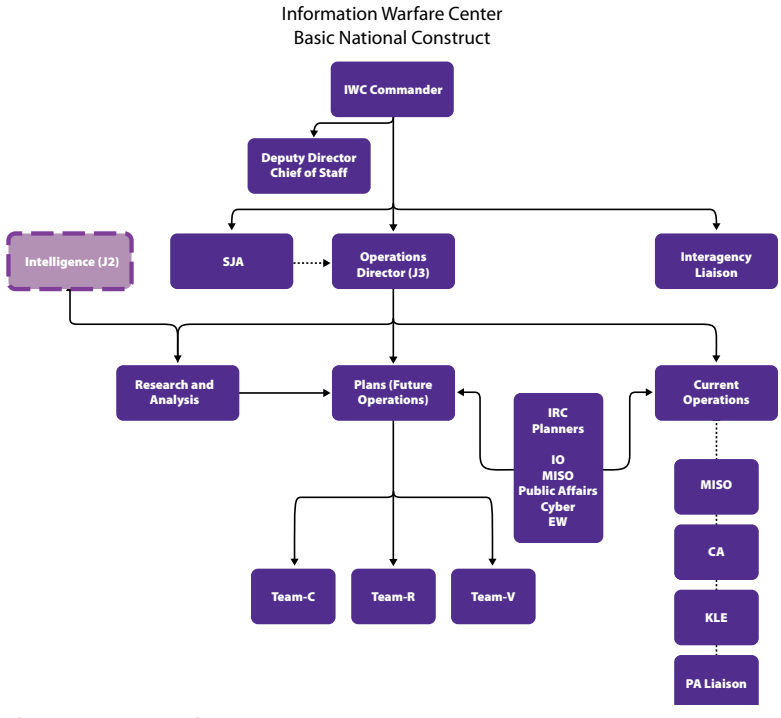

Figure 2. Information Warfare Center notional construct

By designating each TSOC with the supported information command and allocating dedicated resources to an IWC, the DOD would focus the number of supported entities down to six operational-level organizations, establish clear authorities for reach-back, eliminate significant coordination redundancy, increase cross-component synchronization, and reduce information fratricide.

In the reach-back column and operational row of figure 1, the services and functional CCMD provide their subordinate reach-back capabilities to the supported operational components for each CCMD. These reach-back organizations, such as Sixteenth Air Force, bring unique capabilities to the information fight. As geography agnostic organizations, they maintain a global view that balances the regional focus of GCC information supported commands. Supporting only six designated organization, instead of the myriad uncoordinated teams today, would streamline requests for support and clarify engagement authorities.

Interagency Consideration

The DOD can and should present a robust information engagement capability to our nation's leaders. However, we should not be our nation's primary communicator. That responsibility, both by law and sensibility, goes to the DOS. That

said, the DOD currently enjoys a budget 10 times that of the DOS.[7] Much like GCC staffs do not have the capacity to create enough signal-to-noise ratio to impact the IE, the DOS does not have enough resources to engage with prioritized audiences adequately to create sufficient impact. Many embassies have only one US staff member for public affairs and public diplomacy (PAPD), and most of their time is spent on administrative work.[8] Therefore, the DOD could serve as the information engagement framework into which the DOS can plug and play under defense support to public diplomacy. The military's ability to conduct planning and synchronize operations across multiple theaters would dramatically help the overwhelmed DOS PAPD function around the world.

Other Issues

Adopting this framework would be a significant first step in the direction of preparing the DOD to effectively engage in the information domain. However, the other four problem components remain.

Continuing Education for IRC Personnel

Skill levels vary widely between information practitioners and are generally far too low. The future of information warfare will require IE operators to include expertise in data science, sociology, linguistics, machine learning and artificial intelligence, military operational planning, advertising campaigns, communication strategy, and more. Yet, there is no requirement for continuing education in many of the military IRCs. For example, public affairs officers require no additional training beyond their initial technical school to be a CCMD public affairs director.[9] No operational structure can be effective if not staffed by well-trained personnel regardless of how well organized.

Culture Change through Commander Education

Military culture is biased toward physical action by centuries of conditioning—and it shows. We must educate commanders and leaders on IE impacts, planning, and strategy. Strategy is an area with historic developmental shortfalls.[10] Many commanders, but not all, are exposed to strategy but never deliberately learn it and end up as graduated tacticians at higher levels of command. If we fail to train commanders and bring about culture change, information will remain a lesser function despite the Joint Staff designation as one of the seven war-fighting functions.[11]

Interagency Integration

The DOS has the lead for the US in each country, which often frustrates DOD engagement and slows the speed with which the US can engage due to DOS shortfalls. However, it is a reality we must face and overcome through cooperation. Establishing the recommended operational framework will help, but the DOS must also look for ways to refine their own processes and adequately resource information efforts.

Influence Assessment and Visualization

The most technically challenging component of effective information engagement is how to assess and visualize influence. We know how to map physical gains and assess battlefield damage in the military, but we have little idea on how to keep score in the information domain. While the Command and Control of the Information Environment tool is likely a potential long-term solution to this problem (and is getting better), it still needs significant development to fulfill information warfare needs (e.g., have a good, global IE common operating picture, be able to coordinate IE activity, and be able to assess influence of friendly, neutral, and adversary activity).

Conclusion

None of these issues are simple or quick fixes. The DOD and DOS are large bureaucracies with many processes still anchored in post-World War II thinking. The IE is evolving far faster than our traditional culture, organizations, and processes can adapt, so we must make more drastic changes. While the DOD may not adopt the ideas described in this article, I hope it begins a conversation that moves us rapidly forward. Despite the difficulty of the task ahead, I am optimistic we change in time. I choose to be optimistic because the alternative is for the US to effectively cede the entire information domain to adversaries who, unchecked, assail our interests abroad and our citizens at home. So, I choose to believe we can change because my children's future depends on it. ✪

Maj Andrew Caulk, USAF

Major Caulk (BS, USAFA; MS, George Mason University) currently serves as the public affairs director for Special Operations Command Africa. He earned a master's degree from George Mason University in strategic communication.

Notes

1. P. W. Singer, webinar to Air Force Public Affairs, 23 June 2020.
2. National Security Council Strategic Communication and Public Diplomacy Policy Coordinating Committee, *U.S. National Strategy for Public Diplomacy and Strategic Communication* (Washington DC: National Security Council, 2007).
3. Department of Defense (DOD), *Joint Concept for Operating in the Information Environment* (Washington DC: 25 July 2018), https://www.jcs.mil/.
4. DOD, *Joint Publication (JP) 3-0, Joint Operations* (Washington, DC: DOD, 17 January 2017), IV-7.
5. DOD, *JP 3-0,* I-13.
6. Special Operations Command, "Headquarters USSOCOM," accessed 22 January 2021, https://www.socom.mil/.
7. DataLab, *Federal Spending by Category and Agency* (Washington DC: DataLab, 2020), https://datalab.usaspending.gov/.
8. United States Advisory Commission on Public Diplomacy. *Comprehensive Annual Report on Public Diplomacy & International Broadcasting: Focus on FY 2018 Budget Data* (Washington DC: January 2020), https://www.state.gov/.
9. Andrew Caulk, *21st Century Military Strategic Communication* (Fairfax, VA, 2016), 58. George Mason University.
10. Scott Bethel, "Recruiting, Training, and Developing Strategic Thinkers," in Exploring Strategic Thinking: Insights to Assess, Develop, and Retain Army Strategic Thinkers, (Fort Belvoir, VA: US Army Research Institute for the Behavioral and Social Sciences, 2013), 55–65.
11. Thomas Crosbie, "Getting the Joint Functions Right," *Joint Force Quarterly* 94 (3rd Quarter 2019): 96–100, https://ndupress.ndu.edu/.