What Ifs

Building the environment to enable the convergence of information forces

by Capt Paul T. Riggs

Commanders will be most ready to achieve unity of effort in employing information forces by focusing a unit's information planners on individual training and integration into unit exercises. However, this is time-intensive and beset with various complexities. While there is no substitute for experience, we need institutional means to reduce the steep learning curve for commanders and information planners. Two things can equip information planners across the force with the tools to combine multiple information forces during operations: a detailed information objective and an information environment common operating picture (IE COP) populated with enough details to support planners without a background in the specialized information force with which they are planning to converge.

>Capt Riggs is a Cyberspace Officer serving as the Information Environment Current Operations Officer for the Marine Corps Information Command at Fort Meade, MD. He served as the Activation Cell Officer-in-Charge for the command and is currently working with other information environment professionals across the Service to build an information environment common operating picture to better visualize the information environment for action officers and commanders alike. Previous MOSs include Infantry Officer and Aviation Logistics Information Management Specialist.

"In conflicts involving modern militaries, cyberattacks are best used in combination with electronic warfare (EW), disinformation campaigns, antisatellite attacks, and precision-guided munitions. The objective is to degrade informational advantage and intangible assets (such as data), communications, intelligence assets, and weapons systems to produce operational advantage. The most damaging actions would combine precision-guided munitions and cyberattacks to disable or destroy critical targets. Cyber operations can also be used for political effect by disrupting finance, energy, transportation, and government services to overwhelm defenders' decision-making and create social turmoil."

—James Andrew Lewis "Cyber War and Ukraine," CSIS, June 2022

The Case for Convergence

Let us look at two different uses of non-kinetic strikes in coordination with kinetic operations. Before the Russian invasion of Ukraine in 2022, Russian (suspected GRU) cyber actors conducted a series of cyber-attacks targeting the Ukrainian government, non-profit, and information technology systems.[1] These attacks included phishing, website defacement, destructive malware, and distributed denial of service campaigns. While these attacks were numerous, poor coordination with Russian military actions on the ground resulted in insignificant military advantage gained from the cost imposed by the cyber-attacks alone. Furthermore, Russia did little to pair operations with an effort to regain the prevailing narrative following an information campaign conducted by the United States and our allies to "inform domestic and international audiences about Russia's [intent to invade and their playbook]."[2]

Compare the previous example with an Israeli kinetic strike against the Al-Kibar nuclear facility conducted in 2007, known as Operation ORCHARD/OUT OF THE BOX. Intelligence gained from a close-access cyber operation against a senior Syrian official's laptop informed the operational planning for the strike.[3] During the operation, the Israelis allegedly used EW capabilities to gain a foothold in Syrian air defense systems (ADS). This attack enabled cyberspace operators to maneuver through the ADS network and deliver malware, effectively blinding the system. With the ADS unable to detect aircraft, the Israeli Air Force was able to deliver precision-guided munitions to destroy the Syrian ADS radars, enabling freedom of maneuver through Syrian air space for the remainder of the operation.[4] Delivered alone, a hybrid EW and cyberspace attack would have imposed a temporary cost against the adversary. However, timing these capabilities to support a kinetic operation yielded a more significant military advantage.

Background

With the publication of *JP 3-04,*

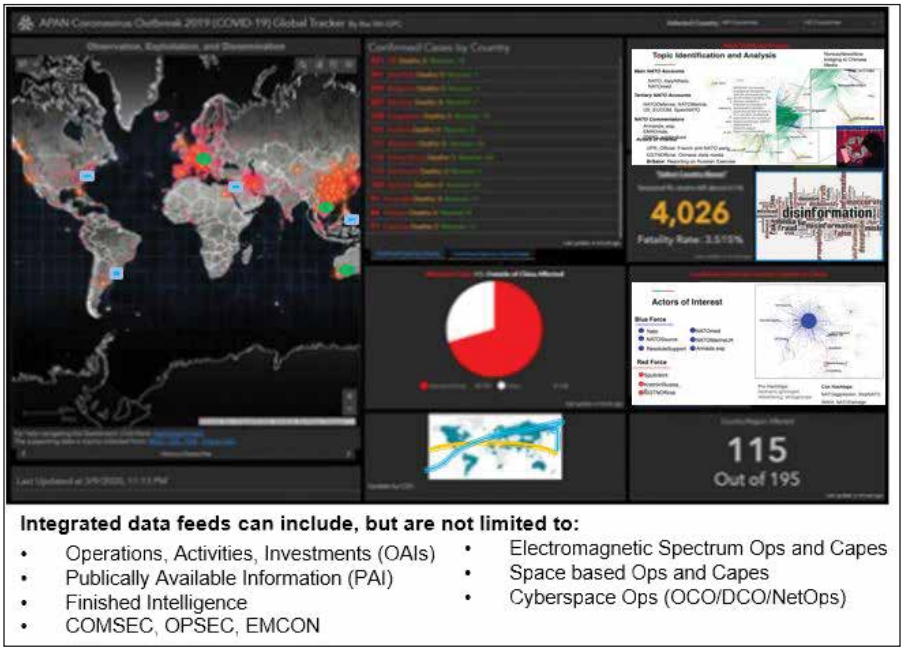
Information in Joint Operations, information forces replace the term information-related capabilities. The term information forces refers to the six capability areas of the information warfighting function: electromagnetic spectrum operations, cyberspace operations, space operations, influence operations, deception operations, and inform operations.[5] The Marine Corps Information Command (MCIC) enterprise comprises commands representative of several information forces under one commander. The commanding general of the MCIC is also the commander of MARFORCYBER, Joint Force Headquarters-Cyber (Marines), Joint Task Force-ARES, and MARFORSPACE. He also serves as the Service cryptologic component commander with the Marine Cryptologic Office and Marine Cryptologic Support Battalion in an ADCON relationship with the MCIC. The Marine Corps Information Operation Center is also assigned to the MCIC.

Since late 2022, when the MCIC activated, a small contingent of Marines and civilians within the command has been working to develop information environment battlespace awareness in coordination with the Deputy Commandant for Information and other information operation cells across the Service. What started as trying to "bind the infinite" of publicly available information across the internet has evolved into building an IE COP. Within the MCIC, the design focus of the IE COP is on supporting information planning and convergence of information forces within the MCIC enterprise by visualizing relevant information in near real-time.

MCIC defines convergence as: "The act of planning for and identifying those processes, synergies, information flow-paths, and complimentary OAIs between commands that maximize collective impact in the information environment in support of a specific objective from the commander."[6] More broadly, this identifies that the combined efforts of two or more information forces can have a more significant effect on the information environment than either could have by trying to achieve the same objective individually. This is similar to the concept of unity of effort at the operational level or combined arms at the tactical level.

"An IE COP must capitalize on available, layered data flows (from network operations, intel, publicly available information, electromagnetic spectrum operations, offensive cyberspace operations, space, friendly/adversary force disposition, weather, significant activities, etc.) to visualize the IE and deliver operational insight visually similar to the doctrinal modified combined obstacle overlay product but as close to realtime as can be maintained. This begins with a geographic display of operations, activities, and investments (OAIs) from friendly/adversary forces and across the information environment."

—John Hoffner "On Information Environment Battlespace Awareness and an IE COP: How an Information Environment Common Operating Picture became an Uncommon Virtue,"
Marine Corps Gazette, ***April 2024***



An example of an IE COP created by the MCIC and presented at the 2023 DC-I Information Summit. ***(Image provided by author.)***

Complexities to Achieving Convergence

Achieving convergence is heavily reliant on the members of the staff. Ideal information planners "have subject matter expertise with specialized capabilities, experience working with and in operations in the information environment (OIE) units, and an understanding of the inherent informational aspects of capabilities and activities of other units."[7] The reality is that most information planners rarely have all these qualities. There are additional complexities common to all staff work and those specific to information forces. These hurdles make convergence planning more challenging and can result in disjointed efforts.

Complexities:

- Each information force is often highly specialized. A cyberspace planner who has historically worked in offensive operations will be less equipped to assist in planning for assured C2 and defensive operations. While this is still better than an unrestricted officer without experience dealing with the authorities' process, the knowledge gap is tremendous. This reduces the capacity for maintaining a working knowledge of the activities of other units, Services, agencies, and partner nations across all information forces.
- As is often the case, any unit will unlikely be at its complete table of organization strength. High turnover rates inherent to the military further stress a staff, which often means a unit's best information planners will depart within months of fully grasping their role.
- Each information force historically operated as a separate entity. Despite recent efforts to merge them into information maneuver, these silos are still present and create barriers. Information forces are accountable to the execution authority and combatant commander that controls them. This results in separate information forces that have requirements to achieve distinct objectives.
- "Military activities that leverage information frequently involve a unique set of complex" authorities and policies.[8] This makes synchronization difficult when the timeline for approvals is vastly different, and each capability requires different processes and authorities to execute.
- There is pressure to preplan responses and/or defenses to potential shifts in geo-political climates and threat actor actions. This additional complexity is sometimes at odds with the actions for campaigning.
- Unlike kinetic fires, non-kinetic fires are global and rarely visible. This makes it challenging to identify adjacent friendly forces operating in a geographic AO and what their efforts are trying to achieve. Coordination is crucial to achieving unity of effort, as operations conducted by one unit may be at direct odds with the efforts a friendly unit, military ally, or partner nation is seeking to achieve.

"Information planners collaborate with the rest of the staff to develop and plan activities in a manner that most effectively leverages the informational aspects of joint force operations, as well as planning OIE, to support achieving the JFC's objectives."

—JP 3-04

Recommendation One: Lead with Information

Leading with information means initiating planning based on a detailed analysis of the effect(s) in the information environment that will achieve the commander's objective. This simplifies the planner's task of solving the right problem and leveraging available resources to reach a solution. Procedurally, this starts by identifying the information objective, ideally informed by substantiating intelligence. In competition, the information objective is often the main effort designed to achieve an isolated effect in the information environment. In conflict, the information objective changes the information environment in a way that gains a military advantage for the rest of the MAGTF. After establishing the information objective, planners collaborate with the rest of the staff to determine which information force and/or capability is best suited to achieve the objective. Planners can identify convergence opportunities by deciding how best to combine available resources to deliver more devastating results against adversaries and more advantageous results for friendly forces. Convergence is no longer the goal but a by-product of good staff work.

Beyond conducting the staff work of mission analysis/problem framing, planners also need to look for external convergence opportunities. Due to the required time to lift efforts off the ground, it would be beneficial to leverage existing authorities of other units that align with both units' information objectives. This differs from capabilities-based planning, in which the planner looks at what they can do and then creates an information objective to match. First, planners identify the commander's objective and break that down into smaller information objectives. Then, the planners review other information forces in the AO and review their information objectives. If anything aligns, planners should begin coordination to pair efforts within all legal boundaries.

Leading with information means initiating planning based on a detailed analysis of the effect(s) in the information environment that will achieve the commander's objective.

Information planners should clearly list their force's information objectives within an online collaborative workspace, such as an IE COP, using an integrated plans-manager tool. The parent command should maintain their campaign plan within their IE COP and associate specific information objectives within the campaign to the information force in support. Not only does this im-

prove the ability to track assessments, but it also enables planners to identify convergence opportunities.

Recommendation Two: Detailed Digital Representation Supports IF Convergence

"To facilitate unity of effort, the ... Commander and supporting staff should be familiar with the roles, expertise, and capabilities of individual and organizational stakeholders relative to the use of information and leveraging information to create relative advantage over an opponent."[9] As mentioned in the list of complexities in the previous section, this familiarization requires a steep learning curve and is difficult to maintain amongst the staff. Improved communication methods make familiarization more accessible. We reduce complexity by putting the responsibility of increasing shared situational awareness on the subject-matter experts at the tactical level.

To simplify communication, we need to contribute meaningful information to an online collaborative workspace (e.g., IE COP) that depicts the total information force laydown in near-realtime and with geospatial tagging. Each subject-matter expert at various commands is responsible for contributing to this IE COP by outlining the information that any planner would need to understand the efforts and composition of available information forces or, at minimum, deconflict actions in the IE.

At a minimum, information forces across the Service should add the capability, limitation, authorities, mission, and the most correct and up-to-date POCs as data points within their digital representation in the IE COP. Some starting requirements are listed in Table 1, with bare minimum requirements underlined.

Subject-matter experts should scope the data points listed in Table 1 to the proper classification level, increasing the amount of descriptiveness at higher classifications. Subject-matter experts should take appropriate measures to avoid any spillage of classified information. Subject-matter experts should also take appropriate measures to get as much information to the force as possible. Additionally, all descriptions must be written in clear English without an overreliance on acronyms or shorthand from the specific information force's niche.

Marines and civilians with Marine Corps Cyberspace Warfare Group and Marine Corps Cyberspace Operations Battalion participate in Cyber Flag 23-2 at an undisclosed location, 7 August 2023. The purpose of the exercise was to enhance readiness and cyber warfare capabilities. Each team was strategically positioned in an offensive or defensive role, engaging with various cyberattack and defense scenarios. ***(Photo by Cpl Oneg Plisner.)***

Section	Description
Capabilities	• Quantity, training, and qualifications of personnel. • List of available equipment with relevant details. • List of effects the unti could conduct. • Adjacent units' capabilities and request process.
Limitations	• Constraints and restraints. • List of relevant laws and policies restricting actions. • List of things that cannot be done by personnel or equipment that would traditionally be capable of this unit. • Timeline-specific impacts (e.g., rotation dates that impact employment)
Authorities	• List execution authority. • List all relevant authorities under which the unit can operate. • Brief description of authorities and their scope. • Duration authorities are valid. • Estimated time for approvals. • Processes/procedures required for approval.
Mission	• Unit mission(s). • Higher HQ's mission. • Known adjacent unit missions (including other agencies, services, or partners).
POCs	• Unclassified and classified points of contact for the operations section responsible for supporting the unit and handling RFSs.

Table 1. Minimum force laydown requirements in an IE COP.

Conclusion

In conclusion, equipping information planners with a detailed objective and a rich IE COP presents a clear path toward achieving unity of effort in information operations. This requires action from various stakeholders, including Joint Force leadership, who must invest in developing and deploying these tools. Information force communities must actively contribute to populating the IE COP with accurate and relevant information. Finally, individual information planners must embrace these resources and continuously hone their

skills to leverage them in operations effectively. By working together, we can unlock the full potential of information forces and ensure our success in the information-age battlefield.

Notes

1. James Lewis, "Cyber War and Ukraine," *CSIS*, June 16, 2022, https://www.csis.org/analysis/cyber-war-and-ukraine.

2. Headquarters Marine Corps, *MCDP 8*, *Information*, (Washington, DC: 2022).

3. Von Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Spiegel International*, November 2, 2009, https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

4. Richard Gasparre, "The Israeli 'E-tack' on Syria–Part II," *Air Force Technology*, March 10, 2008, https://www.airforce-technology.com/features/feature1669.

5. Headquarters Marine Corps, *Joint Memorandum*, *Definitions for Information Related Terms*, (Washington, DC: 2020).

6. This definition comes from a 2023 working group for convergence hosted by the MCIC in Fort Meade, MD. The definition was used to bring elements of the MCIC enterprise together to determine how to proceed with integrated planning.

7. Office of the Joint Chiefs of Staff, *Joint Publication 3-04, Information in Joint Operations* (Washington, DC: 2022).

8. Ibid.

9. Ibid.