2022 LtGen Bernard E. Trainor Military Writing Award Winner: Honorable Mention

Assured C2

Pivoting the 06xx community

by LtCol Arun Shankar

>LtCol Shankar is a CMC Fellow at the Hoover Institution, Stanford University. He has served a combined 28 months in Operation Iraqi Freedom and Operation Enduring Freedom as a counter-IED Analyst, Assessments Analyst, and Communications Officer, and holds a PhD in Operations Analysis from George Mason University, Fairfax, VA.

At present, the role of the 06xx communicator is primarily focused on operating and maintaining equipment. The highly dynamic and technical nature of this occupational field (occfield) has previously allowed little room for responsibilities beyond the fundamental activities of network storage, transport, and security. However, the consolidation of this complexity to cloud network management, commercial satellite service rentals, and web-based software applications will transform this setting.

Moreover, today's communicators are charged with the overarching responsibility of *Assured Command and Control (C2)*—setting the optimal conditions for a commander to issue orders, receive feedback, and make decisions. Consequently, network capabilities only cover only a fraction of this task. The management of knowledge and information also underpins this definition, but communicators do not yet embrace this role.

The combination of these emerging circumstances requires a significant adaptation of our occfield. In particular, manpower gained from centralized and outsourced capabilities can be shifted to information management, truly fulfilling the mission of Assured C2. The subsequent sections further develop this premise.

Current State

Assured C2. Command is the lawful authority and influence a commander has over his subordinates; control is the feedback loop that occurs between the issuance of the commander's orders and the assessment of their effect. Of these two elements, *assured control* should most interest communicators. Control can be boiled down to a science and largely delegated to a staff for action. Information and knowledge management drive the feedback loop that creates Control.

Following this logic, the assurance of control, through information management, goes far beyond the mere provision of a tactical network. The goal of information management is to create knowledge and shared understanding, eventually leading to the end state of decision making. This is done through the advancement of raw data along a cognitive hierarchy, using filters and fusion within the staff. It includes the establishment of battle rhythms, reports requirements, meaningful staff collaboration, and data management. Specifically, this management includes the storage, categorization, analysis, manipulation, and transit of the data. At present, communicators largely only focus on storage and transmission, passively enabling C2 but *not* actively assuring it.

Network consolidation. The consolidation of cloud storage, network infrastructure, data centers, and application servers is emerging across all three MEFS. Today, when units exercise or deploy, they often reach back to the local communications battalion for these services rather than build them from scratch in the field. Moreover, some units even temporarily procure these capabilities *as-a-service*, where setup and maintenance are centralized and outsourced to commercial vendors. As a result, few units build servers anymore, relegating many data systems administrators to helpdesk tasks focused on user account paperwork and the configuration of end-user devices. The same is true for transmission systems operators in units where satellite communications are procured as-a-service.

The emergence of the Marine Corps Enterprise Network (MCEN) in field environments has reinforced this centralization effort. The MCEN contends to be the single network solution, with a seamless user transition from garrison to deployed environments. This cloud capability significantly reduces the complexity of server architectures in the field, shifting this burden to predominantly civilian organizations that are better trained and resourced for this role. Upcoming tactical exercise testing and experimentation will likely iron out the remaining hurdles in this endeavor.

This reliance on resilient satellite links for cloud reachback has been criticized because it cannot be depended upon during high-intensity phases of warfare. During these periods, enemy forces will

likely jam and/or geolocate these satellite signals, reducing their ability to transmit data. However, most regimental-sized units have adapted to this challenge, relying on resilient, line-of-sight radio networks in the absence of full mesh secure and non-secure internet. Consequently, short-burst communications are, once again, becoming an adequate method of controlling a unit.

Kill chains. Information flows along a kill chain, from *sensor* to *shooter*. A sensor draws raw data from the operating environment. Examples can include an intelligence asset, an aerial reconnaissance platform, a social media site, or a forward observer. A shooter places an effect on a target, whether it be kinetic or non-kinetic. A kill web is a two-dimensional kill chain with multiple sensors and shooters, forming a web of exponentially greater options for a commander.

Communicators are charged with enabling the shortest kill chains to commanders, where length is determined by time, not physical distance. The kill chain is akin to the OODA loop, where commanders observe and orient (sense), then decide and act (shoot). This model is conceptually synonymous with information management, where data is collected and processed into information, knowledge, and wisdom (sense), then presented for a decision (shoot).

Presently, communicators see kill chains as strings of transmissions systems, firewalls, network switches, routers, servers, and end-user devices that allow the efficient and reliable flow of information, but they do not see a role in optimizing and processing the information itself. Instead, this secondary role is stovepiped among the various warfighting functions in the kill chain, likely without oversight or synchronization, resulting in inefficiency, suboptimal tempo, and subpar decision making.

Information Environment. The newly established warfighting function of Information, as certified by the release of *MCDP 8,* includes cyber, space, and influence operations. Specific MOSs in the 17xx occfield were already established to tackle the tasks within these missions. The cyber-MOSs are focused on offensive and defense cyber operations, the space MOSs are dedicated to space control activities, and the influence MOSs are rebranded combinations of the former psychological and information operations. However, the mission of Assured C2 remains with the 06xx community. It neatly serves as the foundation for all warfighting, to include information maneuver and its subcomponents; the information feedback loop that underlies control is the essence of decision making. For this reason, Assured C2 is the most vital component of the information environment.

The "iron mountain" of C2 equipment, once required to operate and manage information, is being replaced by lighter, more capable systems. *(Photo by Sgt Jacob Wilson.)*

Future State

The 06xx occfield should capitalize on the opportunities that lay ahead. First, the community must accept the emergence of commercial, *as-a-service* solutions for tactical networks and embrace the opportunity to export network complexity to an outsourced solution. This includes the use of the MCEN as the warfighting network in tactical environments. Our MEFs are already poised for this transition, as they have each now centralized domain ownership within the senior communications node. The MCEN still needs to prove ready and regular responsiveness to helpdesk matters, and it must allow flexible network permissions to appropriate leaders at the tactical edge. Further experimentation should be conducted during full-scale GCE exercises, where network complexity and friction are at their highest. Once this is achieved, the MCEN should be adopted as the warfighting network. Without the MCEN fully serving its central purpose, efforts to run tactical networks continue to be duplicated at each MEF, creating a manpower tax that prevents investment in vital assured C2 and information management roles.

Second, the force structure gained from these outsourced solutions, particularly within the 067x community, should become information managers. These Marines should be trained in the use of data categorization, manipulation, and analysis tools, as well as basic application development. This includes a familiarization of popular C2 applications that provide the common operational picture, chat messaging, and fires deconfliction. These Marines must have a cursory understanding of staff processes and have a curiosity for owning and improving these processes without being summoned to do so. The newly formed 0673 application developer MOS can likely serve this purpose.

Third, communications chiefs should be introduced to staff processes, information management, and modern data science tools in career-level training. Without this, S-6 shops will fail in this mission, depending solely on the

enthusiasm of a young company-grade or field-grade officer to drive this effort. Information management is as much art as it is science, and it requires an understanding of people and culture, largely gained through years of experience, to ensure success. Our senior enlisted leaders provide this function.

Lastly, officers holding the 0602 MOS should be skilled in the true meaning of Assured C2, fully grasping the underlying concepts of staff roles and responsibilities, shortening kill chains, and optimizing decision making. They should also have a basic understanding of data science and associated software tools. Within C2, these officers should be focused on control, rather than command, since this is the element of C2 that is chiefly owned by the staff. This role goes beyond equipment strings; it requires a strong understanding of all seven warfighting functions and how a staff works to help a commander make decisions. Additionally, this G-6/S-6 officer should have the authority to optimize this information flow across the staff.

In this future state, communicators would be responsible for establishing the entire staff's battle rhythm, ensuring huddles and meetings are optimally scheduled to enhance and refine information flow. Collaboration would be planned and outlined prior to execution. Reports would be formatted, transmitted, and stored efficiently. The staff would use C2 applications interactively, with appropriate permissions and ground rules set by the G-6/S-6. Customized applications and spreadsheet tools would be developed by the G-6/S-6 to assist with this fusion. Data conditioning and curation could be delivered in hours or days rather than through the current, multi-year acquisition process. Automated tools would mine free text reports for data correlations across all warfighting functions. For instance, a tool might be developed to scour all safety incident reports from the last year, discovering a correlation between a lack of tactical vehicle training (G-4), inaccurate map data (G-2), and unserviceable tactical radios (G-6).

Marines in the 062x and 063x fields would continue establishing and maintaining the transport layer of tactical networks. This includes local area switches, both wired and wireless. It also includes satellite terminals (when not outsourced), as well as the employment of single-channel radios, particularly during times of degraded communications. Fully trained 0671s could provide manpower to the MCEN hubs and spokes, while 0673s could serve as information managers under G-6/S-6 leaders, enhancing information flow and decision making across entire command staffs. In this manner, Assured C2 would be met in its fullest meaning.

... mobile, lightweight footprints that reach back to server farms and data centers are now becoming customary.

Concluding Remarks

Remaining in our current state is not an option. The burdensome, iron mountain tactical networks that we haul to the field and establish as our own zip code will no longer support the demands of our Corps. Instead, mobile, lightweight footprints that reach back to server farms and data centers are now becoming customary. Moreover, an aggregated cybersecurity effort at the Marine Corps Cyber Operations Group is much preferred over our ailing, haphazard security efforts in the field. This is best accomplished with one network—the MCEN.

Contrarians have also resisted commercial cloud and satellite solutions to tactical networks under the premise that they would not be reliable during a high-intensity conflict. This would likely be true inside the weapons engagement zone of the conflict, but not outside of it, where much of the decision making is happening. Tactical commanders inside the weapons engagement zone are trained and prepared to use resilient, line-of-sight links to pass critical information during short, designated time intervals. The consistent need for large data pipes at these positions is no longer expected or justified.

Moreover, the longstanding resistance to inheriting the role of information management in the 06xx community must end. Chiefs of staff and executive officers are overwhelmed with modern legal and administrative obligations and, therefore, cannot also ensure effective information management throughout the staff. Assigning the task to a short-timer in the G-3/S-3 is also no longer sufficient. The role must be adopted by a primary staff officer that understands all warfighting functions with the skills and authority to impact the commander's decision making. This is especially important as we adopt *Force Design 2030* and the *Commandant's Planning Guidance*, where decentralized control underpins nearly every premise. The 06xx community is poised to take on this role.

Furthermore, a full inheritance of information management, killchains, and tactical network transport reinforces our occfield's status as warfighters, not just enablers. Success in this future environment demands a holistic understanding of MAGTF operations, building more versatile leaders within our MOS community. This, in turn, could lead to higher retention and better opportunities for career advancements. The time is right to make this bold, but necessary, change in our community.

>Author's Note: Credit is due to BGen Joseph Matos for sharing his thoughts on the future of our occfield. I equally thank Col Joe Broome for his fierce position on reenergizing our community. Lastly, thanks to my dear friend, LtCol Charlie Bahk, for his efforts in developing the 0673 MOS and blazing a trail for its future.

USMC