Adapt or Perish: A Call to Revise the Marine Corps' Command, Control, Communications, and Computer (C4) Architecture

Captain Olaolu N. Ogunyemi

USMC

Major Blaine Ballard--CG 13

January 28, 2022

In 1945, Herbert George Wells wrote, “adapt or perish, now as ever, is nature's inexorable imperative.”[1] This quote is exceptionally germane to the Marine Corps’ assessment and subsequent actions required to adequately prepare for peer competitors. Over the past two decades, counterinsurgency operations against a less capable enemy decreased the need for rapid advancements in the cyberspace domain; however, when considering a peer adversary, “U.S. military superiority is no longer assured and the implications for American interests and American security are severe.”[2] Therefore, the Marine Corps must act expeditiously to prepare for future engagements with peer competitors. The Marine Corps must immediately divest legacy equipment and procure innovative technology, develop a comprehensive signature management plan, and reduce the cyberspace threat surface by developing a shared enterprise C4 architecture.

The first immediate change requires a complete review of current Marine Corps C4 assets and capabilities. Former Deputy Commandant of Information, Lieutenant General Lori Reynolds stated, “the network that the Marine Corps needs must provide interoperable, ubiquitous, and rapid/agile access to information and data [and] equipment used for the last twenty years in Afghanistan and Iraq will not stand up to a peer adversary with capabilities in all warfighting domains.”[3] Throughout history, the Marine Corps has relied heavily upon receiving accurate and timely data to improve processes and inform decisions. Emerging technologies provide the means to record, store, and disseminate data while reducing manual errors; errors that could cause casualties due to inaccurate or outdated information. Contrarily, the Marine Corps employs a “complex and fragmented” C4 architecture that mixes disparate legacy and digital capabilities that are often incompatible.[4] This incompatible mix degrades the information exchange process

by increasing the time required to access data while decreasing the accuracy and reliability of the data.

Addressing this discrepancy requires the Marine Corps to divest of legacy equipment and purchase innovative technology. LtGen Reynolds accurately assessed that the Marine Corps must procure and, "[leverage] emerging capabilities such as Next Generation Troposcatter, enhanced Wideband SATCOM, and Free Space Optics."[5] These capabilities, and others like them, provide secure digital links between two nodes and are updated to counter peer adversary capabilities. Thus, the Marine Corps should prioritize purchasing and distributing next generation technology to out cycle the enemy. This technology should integrate into the pre-existing electromagnetic baseline that exists in heavily contested areas. For example, over the past four decades, numerous multinational corporations have established a presence in key areas in the Pacific region.[6] The Marine Corps should examine these corporations' network infrastructure to identify best practices for sustained Expeditionary Advanced Base Operations. Once examined, the Marine Corps should develop a resilient, ubiquitous, and indistinguishable C4 architecture. Failure to do so will undoubtedly result in C4 disparities across the organization and will accentuate Marine Corps operations in the electromagnetic spectrum revealing tactical actions to peer adversaries.

The negative effects of revealing tactical actions have been highlighted in several Marine Corps force-on-force exercises. Even so, some would argue that there is an adequate amount of emerging technologies at the tactical edge. This claim is supported by articles like "Communications Planning, Execution, and Assessment during STEEL KNIGHT-20" in the *Marine Corps Gazette*. For example, Lieutenant Colonel Arun Shankar & Chief Warrant Officer 3 Emedin Rivera recounted in their article that 7th Marines employed the Kymeta antenna; an

on-the-move satellite communications system that can achieve a reliable data throughput that far exceeds the Marine Corps Network On the Move (NOTM) capabilities.[7] Though true, emerging technology is too-often procured at the Command Element-level. This creates a C4 disparity between the different elements of the Marine Air Ground Task Force (MAGTF) while further segregating the Marine Corps C4 architecture. In an information paper, the 1st Marine Logistics Group (MLG) Assistant Chief of Staff G-6 outlined some of the cons associated with an uneven distribution of critical C2 technology throughout the MAGTF. This includes precluding elements of the MAGTF from meeting Marine Expeditionary Force Operations Plan information exchange requirements.[8] Therefore, continuing to independently procure emerging technology will further exacerbate the negative effects of an incompatible C4 architecture.

The incompatibilities in the C4 architecture inadvertently detract from signature management (SIGMAN) efforts. Over the past two years, the Marine Corps released SIGMAN guidance via Standard Operating Procedures (SOP) and handbooks while adopting quotes like, "to be detected is to be targeted is to be killed."[9] However, because the Marine Corps' efforts to implement SIGMAN are in their infancy, leaders across the organization have not fully implemented SIGMAN to its fullest. Some may mistake Marine Corps commanders' mastery in reducing physical signatures (visual, infrared thermal, and radar) for mastering SIGMAN concepts overall. Meanwhile, units across the Marine Corps have given little thought to controlling their technical and administrative signatures, and the newly developed service-level SOPs and handbooks mark the first of their kind and have not yet been distributed to and implemented by commanders. Therefore commanders have continued to employ outdated tactics, techniques, and procedures (TTP) that are inadequate for future operations against a peer adversary. These outdated TTPs were documented in the MAGTF Exercise (MWX) 1-21 After

Action Report (AAR) published by the Marine Corps Red Team (MCRT), Marine Corps Cyber Operations Group.

During MWX 1-21, the MCRT acted as an adversary force in the cyber domain using a three-phased approach: initial foothold, network propagation, and actions on objective.[10] A preponderance of the MCRT's tactical success was a direct result of abysmal administrative SIGMAN efforts. For example, the MCRT, "retrieved improperly discarded unclassified information from waste containers, including vehicle convoy schedules, equipment custody records, and rosters of [exercise force (EXFOR)] personnel."[11] This information provided a targetable list of personnel for subsequent phishing attacks. Using the phishing attacks, the MCRT gained access to the EXFOR's data network. Once they had network access, MCRT "operators exfiltrated information from an EXFOR file share. Enabling the [MCRT operators] to positively identify and target EXFOR positions with notional kinetic and non-kinetic effects."[12] This is just one of many examples of how a peer adversary may use poor Marine Corps SIGMAN practices to conduct kinetic and non-kinetic actions.

Considering the aforementioned, the Marine Corps should immediately adopt, disseminate, and evaluate a standard/more robust signature management framework designed to instruct commanders on how to manipulate, control, and assess risks associated with their respective unit's signatures. Commanders should hastily integrate the current and forthcoming service-level SIGMAN handbooks and conduct bottom-up refinement on these products. Concurrently, the service should develop evaluation and inspection criteria to assess, improve, and standardize the procedures used Marine Corps-wide to implement SIGMAN concepts. These inspections should be weighted and prioritized similar to the Field Supply and Maintenance Analysis Office assessment program or the Commanding General's Inspection Program. The

Marine Corps will only experience significant progression when SIGMAN concepts become priority.

Significant progression becomes paramount as the Marine Corps continues to prepare for peer adversaries. According to the Marine Corps Strategy for Assured Command and Control, "adversaries use both simple and sophisticated methods designed to reduce the Marines' [C2] effectiveness. This requires a fundamental change in the way Marines create, share, disseminate, and store information across the battlefield."[13] This fundamental change begins with the combatant commanders' thorough and honest assessment of the information exchange required to efficiently C2 forces. Commanders should limit systematic or real-time information exchange requirements and reduce the overall information load for troops at the tactical edge. This emphasizes the need for the Marine Corps to strictly adhere to one of the most basic tenets of maneuver warfare: enable decentralized control using a clear, well-nested commander's intent. This is not the current case. In fact, the Marine Corps continually uses cumbersome C2 applications that require constant connectivity for information exchange (e.g. Global Combat Support System-Marine Corps). Nonetheless, the goal should be to deliver the most critical information at the right time in the right context.

Once commanders narrow down information requirements, the Marine Corps must develop a shared enterprise C4 architecture. This will require a major overhaul and adjustment from the Marine Corps' current model—employing several disparate tactical networks across the organization.[14] As the Marine Corps develops the shared C4 architecture, leaders at the tactical edge must fully understand their role in planning, installing, securing, operating, and maintaining (PISOM) their area of operation within the newly-consolidated cyber battlespace. This requires adequate training. Currently, Marine Corps Communications professionals' minimum

requirements pale in comparison to their U.S. Army counterparts. For example, the U.S. Army signal officer must have at least four years of experience or two years of experience with advanced degrees in a related field in the following areas: Information Technology (IT) Management, Project Management, Information Technology Infrastructure Library (ITIL), Agile development, Cybersecurity, IT Equipment Procurement, and IT Helpdesk Management. Additionally, The U.S. Army prefers the following qualifications: ITIL certifications, Project Management Professional (PMP), and Certified Information Systems Security Professional (CISSP).[15] Though these industry certifications exist to develop robust and secure IT infrastructures internationally, these requirements simply do not exist in the Marine Corps which degrades its Officers' ability to effectively lead Marines as they PISOM their cyber area of operations. This is a training and education deficiency that the Marine Corps must immediately address or risk significant casualties as a result of poorly planned operations in the cyber warfighting domain.

Many may argue that the Marine Corps has already made significant progress preparing for operations in the cyber warfighting domain. In fact, the Marine Corps recently shared the USMC Enterprise Network Modernization Plan.[16] This plan does an excellent job of defining the future network requirements and matching Lines of Effort to time-based phases. Upon initial review, one may assume these changes adequately prepare the Marine Corps for a future conflict with a peer competitor. However, this 291-page plan lacks fidelity. For example, phases are associated with fiscal years instead of exact completion dates. More importantly, there are no tasks directed to operational forces. This creates a clear and inevitable divide between the network modernization planners and the Marines who execute the mission at the tactical edge. Network modernization planners should conduct integrated planning with Marines from the

operating forces and ensure units across the Marine Corps fully understand their part in consolidating the C4 architecture and preparing for the future fight. Failure to do so will stagnate Marine Corps efforts to rapidly flex to forthcoming requirements.

History has shown that the Marine Corps must remain flexible to continue to be the nation's force-in-readiness. Failure to adapt leads to casualties, or worse, fatalities. Therefore, as the Marine Corps shifts focus to maritime operations, the aforementioned steps will ensure it maintains operational and strategic advantage in future contingency operations. It is imperative that the Marine Corps maintains awareness of its adversaries' capabilities and develop a counterbalanced C4 architecture. The Marine Corps' survival and success hinges on its ability to rapidly adapt to the ever evolving nature of war. Thus, the Marine Corps must expeditiously implement the required changes or become extinct.

Notes

[1] Wells, H. G. 1945. *Mind At The End Of Its Tether.* Kingswood: Windmill Press.

[2] Commission on the National Defense Strategy for the United States. (2018). *Providing for the Common Defense.* Washington D.C.: United States Institute of Peace. Retrieved from https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf

[3] Headquarters Marine Corps Deputy Commandant, Information . 2021. *(CUI) DRAFT United States Marine Corps Enterprise Network Modernization Plan.* Quantico: Headquarters Marine Corps Deputy Commandant, Information, Page iii.

[4] Department of Defense. 2020. *Command, Control, and Communications (C3) Modernization Strategy.* Washington D.C.

[5] Headquarters Marine Corps Deputy Commandant, Information . 2021. *(CUI) DRAFT United States Marine Corps Enterprise Network Modernization Plan.* Quantico: Headquarters Marine Corps Deputy Commandant, Information, Page iii.

[6] Fairbairn, Te'o I. J., and Thomas T. G. Parry. 1986. "Multinational enterprises in the developing South Pacific region." *International Business Enterprises-Oceania*, 85.

[7] Shankar, Arun, and Emedin Rivera. 2020. "Communications Planning, Execution, and Assessment during STEEL KNIGHT-20." *Marine Corps Gazette* WE56-WE59.; Kymetta Corporation. 2019. "Product Sheet-Kymeta." *ST Engineering.* Accessed October 20, 2021. https://www.idirect.net/wp-content/uploads/2020/03/ProductSheet-Kymeta-u7-Terminal.pdf.

[8] Woulfe, James, and Olaolu Ogunyemi. 2021. *TABLE OF ORGANIZATION AND EQUIPMENT CHANGE REQUEST (TOECR) FOR 1ST MARINE LOGISTICS GROUP, ALPHA TAMCNS: A03367G, A02167G, A020117G.* Information Paper, Oceanside: 1st Marine Logistics Group.[4] Guthrie, Katherine. 2021. *SIGNATURE MANAGEMENT BASELINE ASSESSMENT AND FRAMEWORK DEVELOPMENT.* Position Paper, Oceanside: 1st Marine Logistics Group.

[9] HEADQUARTERS UNITED STATES MARINE CORPS. 2016. *The Marine Corps Operating Concept.* WASHINGTON, D.C: DEPARTMENT OF THE NAVY.

[10] Marine Corps Red Team, Defensive Cyberspace Operations Division. 2020. *MARINE CORPS RED TEAM AFTER ACTION REPORT FOR OPERATION 21-06.* After Action Report, Quantico: Marine Corps Cyberspace Operations Group, Page 3.

[11] Marine Corps Red Team, Defensive Cyberspace Operations Division. 2020. *MARINE CORPS RED TEAM AFTER ACTION REPORT FOR OPERATION 21-06.* After Action Report, Quantico: Marine Corps Cyberspace Operations Group, Page 2.

[12] Marine Corps Red Team, Defensive Cyberspace Operations Division. 2020. *MARINE CORPS RED TEAM AFTER ACTION REPORT FOR OPERATION 21-06.* After Action Report, Quantico: Marine Corps Cyberspace Operations Group, Page 5.

[13] HEADQUARTERS UNITED STATES MARINE CORPS. 2017. *Marine Corps Strategy for Assured Command and Control.* Washington, D.C.: Department of the Navy.

[14] Russell, J. M. (2020). *Command and Control in Maneuver Warfare: Transition to the Marine Corps Enterprise Network.* Quantico: Marine Corps University.

[15] United States Army. 2016. *Talent Management.* Accessed December 13, 2021. https://talent.army.mil/job/signal/.

[16] Headquarters Marine Corps Deputy Commandant, Information. 2021. *(CUI) DRAFT United States Marine Corps Enterprise Network Modernization Plan.* Quantico: Headquarters Marine Corps Deputy Commandant, Information

Bibliography

Commission on the National Defense Strategy for the United States. (2018). *Providing for the Common Defense.* Washington D.C.: United States Institute of Peace. Retrieved from https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf

Department of Defense. 2020. *Command, Control, and Communications (C3) Modernization Strategy.* Washington D.C.

Fairbairn, Te'o I. J., and Thomas T. G. Parry. 1986. "Multinational enterprises in the developing South Pacific region." *International Business Enterprises-Oceania*, 85.

Headquarters Marine Corps Deputy Commandant, Information . 2021. *(CUI) DRAFT United States Marine Corps Enterprise Network Modernization Plan.* Quantico: Headquarters Marine Corps Deputy Commandant, Information .

HEADQUARTERS UNITED STATES MARINE CORPS. 2017. *Marine Corps Strategy for Assured Command and Control.* Washington, D.C.: Department of the Navy.

—. 2016. *The Marine Corps Operating Concept.* WASHINGTON, D.C: DEPARTMENT OF THE NAVY.

Kymetta Corporation. 2019. "Product Sheet-Kymeta." *ST Engineering.* Accessed October 20, 2021. https://www.idirect.net/wp-content/uploads/2020/03/ProductSheet-Kymeta-u7-Terminal.pdf.

Marine Corps Red Team, Defensive Cyberspace Operations Division. 2020. *MARINE CORPS RED TEAM AFTER ACTION REPORT FOR OPERATION 21-06.* After Action Report, Quantico: Marine Corps Cyberspace Operations Group.

Russell, J. M. (2020). *Command and Control in Maneuver Warfare: Transition to the Marine Corps Enterprise Network.* Quantico: Marine Corps University.

Shankar, Arun, and Emedin Rivera. 2020. "Communications Planning, Execution, and Assessment during STEEL KNIGHT-20." *Marine Corps Gazette* WE56-WE59.

United States Army. 2016. *Talent Management.* Accessed December 13, 2021. https://talent.army.mil/job/signal/.

Wells, H. G. 1945. *Mind At The End Of Its Tether.* Kingswood: Windmill Press.

Woulfe, James, and Olaolu Ogunyemi. 2021. *TABLE OF ORGANIZATION AND EQUIPMENT CHANGE REQUEST (TOECR) FOR 1ST MARINE LOGISTICS GROUP, ALPHA TAMCNS: A03367G, A02167G, A020117G.* Information Paper, Oceanside: 1st Marine Logistics Group.