Beans, Bullets, Band-Aids ... and Bytes?

Networking as digital logistics

by Capt Olivia A. Garard & Maj Craig M. Schnappinger

> ***Strategy is to war what the plot is to the play; Tactics is represented by the role of the players; Logistics furnishes the stage management, accessories, and maintenance.***
>
> ***—LtCol George Cyrus Thorpe***

>Capt Garard is an Unmanned Aircraft Systems Officer assigned to the Ellis Group who wrote this article while serving with Task Force Southwest in Afghanistan.

>>Maj Schnappinger is the Communications Officer for 2d Marine Regiment, currently serving as the Assistant Chief of Staff J-6 for Task Force Southwest 19.1 in Afghanistan.

Logistics is the stuff of war. It is the means through which battles are fought and wars are won, or all too often lost. It is more than the material itself, but having the right resources, at the right time, and in the right place. *MCDP 4, Logistics* explains, "Logistics provides the resources of combat power, positions those resources on the battlefield, and sustains them throughout the execution of operations,".[1] The required resources evolve with the mercurial character of warfare. As the Prussian master observed, "The necessity of fighting very soon led men to special inventions to turn the advantage in it in their own favour."[2] Some *special inventions* change the degree of combat power, like the difference between the Gatling gun and the M240B. Others change the kind of combat power, like those offered by digital technologies. Regardless, each requires an evolution in logistics: moving elements however, whenever, and wherever they are needed. To fully leverage 21st century capabilities, we need to resource the logistics of the digital age.

In 1998, VASM Arthur K. Cebrowski and John J. Garstka wrote "Network-Centric Warfare—Its Origin and Future." They foresaw a shift from prioritizing the platform to emphasizing the connections between components, agents, and sensors. As they explain, "*Network-Centric Warfare* derives its power from the strong networking of a well-informed but geographically dispersed force."[3] Their focus is on the conceptual connections between disaggregated sensors and shooters and the corresponding information flow. In the book, *Network Centric Warfare: Developing and Leveraging Information Superiority*, David S. Alberts, John J. Garstka, and Frederick P. Stein acknowledge the importance of the "backplane" and the "information infrastructure or 'infostructue'" required to facilitate the transfer of information, but they relegate those concerns to the "purview of technologists."[4] They gloss over the networking and neglect the logistics. Network-Centric Warfare may not live up to all of its sweeping conceptual claims of being "the most important RMA [revolution in military affairs] in the past 200 years," but what Cebrowski and Garstka initially proposed is increasingly com-

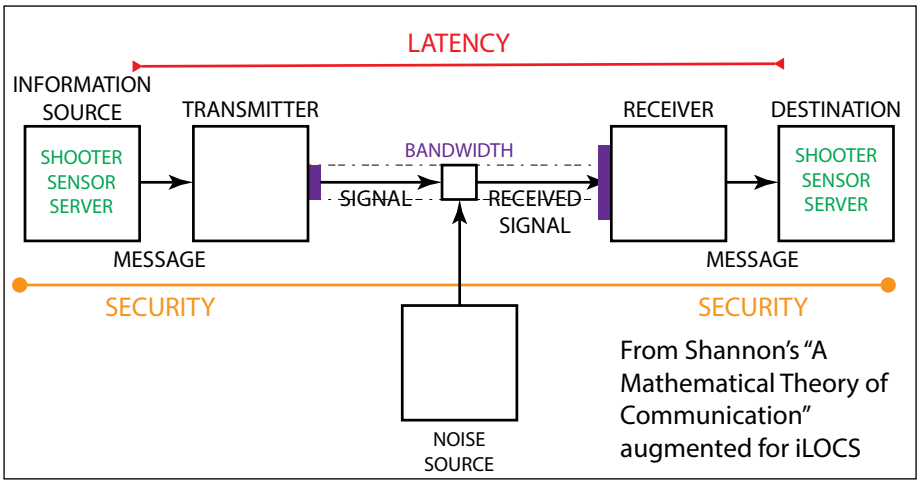

Figure 1.

ing to fruition. Consider that for many years now networked aircraft remotely piloted from the continental United States have found and destroyed more of our nation's enemies than the entire traditionally manned, non-networked, and locally flown aircraft—including as part of close air support missions.[5]

To fully exploit networked interconnected combat power, we need to pay due diligence to what Cebrowski and Garstka omitted: the physical and non-physical requirements to move information between sensors, shooters, and actors.[6] Here, we reach a convergence between *MCDP 6, Command and Control* and *MCDP 4, Logistics*. The flow of information—the means of command and control (C2)—now delimits "*what is operationally possible.*"[7] The physical capacity to transmit information informs the kinds of tactics we can employ and the range and scope of our capabilities, what *MCDP 4, Logistics* describes as "the style of war."[8] Our style is determined by our proficiency filtered through our "commitment to [our] own intent," which is maneuver.[9] Given the ability to transmit information between numerous diverse and dispersed sensors and shooters, we enhance our capabilities to apply our combat power in accordance with our maneuver warfighting philosophy.[10] The multiplicity of options enable us to reach a higher level of maneuver: maneuver in space, in time, and in combination.

Networked combat power derives from the permutations and combinations of disaggregated shooters and sensors. But the source of that power is in the fact of the connection, not in any one node; rather, it is the sensors and shooters connected together. "Dispersed formations" MG Robert H. Scales, USA(Ret), claims, "can only be kept cohesive and capable of massing on demand if a robust cyber network ties them together."[11] A robust network, however, does not imply continuous connections, just a resilient potential for connectivity. It is untenable, imprudent, and tactically inefficient to remain connected at all times. What matters is that the nodes can—meaning that it is physically and logically possible—transmit information between sensors and shooters. This is a weaker claim, but sufficient to deliver combat power when and where it's needed. The multiplicity of connections increases the resiliency of our network, amplifies our possible combat power, and provides a way to distribute our forces throughout the world without dissipating our capabilities.

Whether or not this network, in support of distributed formations, enables the massing of forces or the massing of effects,[12] the possibility for coordination and synchronization of resources and forces will be the limit of combat power. Understanding the absolute—in the capital-A Clausewitzian-sense—limit is important, but that does not help us "to extend those limits as far as possible," as *MCDP 4, Logistics* reminds us.[13] To do that we need to dig into the nuts and bolts, or better yet, the bits and bytes that makes our network possible. We also need to couple this with an honest appreciation that the battlefield is global and extensive; we can no longer circumscribe the fight and all its supporting elements to an area.[14] The battlefield is persistent and pervasive, this requires a holistic, practical understanding of the expeditionary network needed that is balanced by what is logically and physically possible.

A robust network, however, does not imply continuous connections, just a resilient potential for connectivity.

Still, logistics circumscribes the possibilities. As Lieutenant Colonel George Cyrus Thorpe underscores in *Pure Logistics: The Science of War Preparation*, "It is not only necessary to decide what is desirable, but what is possible."[15] Options in the digital space are constrained by the enduring obstacles of "time, distance, and terrain," as well as cost.[16] What varies is the scale and the speed, not the nature of the problem: constructing and securing lines of communication. "Lines of communication," Clausewitz explains, compose "the connection between the army and its base, and are to be considered as so many great vital arteries."[17] Though Clausewitz was referring to roads in *On War*, the concept extends to all domains, such as sea lines of communication (SLOC) or air lines of communication (ALOC). Like arteries, they are as vital as they are vulnerable.

Information also requires a line(s) of communications. It is ironic that line of communication contains the word "communication," while that element has been divorced from the concept.[18] During the Napoleonic era, the road that connected an army to its base was also the path along which a courier would travel. A line of communication as a pathway for communication was implicit. Given the proliferation of digital technologies and our reliance on them, this pathway must be explicit, like a data transmission circuit which includes the transmission media and equipment. Nor does it necessarily follow the same pathways as other LOCs.[19] Information lines of communication (iLOC) are the data transmission circuits along which data flows, including satellites, fiber optic cables, and their critical components such as routers, servers, encryption devices, and radios. In a network, iLOCs function as numerous, distributed capillaries as well as a few vital arteries.

"The fundamental problem of communication," writes the father of information theory, Claude Shannon, "is that of reproducing at one point either exactly or approximately a message selected at another point."[20] This is the difference between *good readback* and *say again*. Tackling this problem serves as the underlying motivation for the Marine Corps' strategy for assured C2: achieving a unified, expeditionary, resilient, and, of particular importance, interoperable network.[21] A unified architecture is consistent with the *National Defense Strategy's* appraisal that we are in persistent competition within the contact layer, because the network, the Global Information Grid, and the internet *is* part of the contact layer.[22]

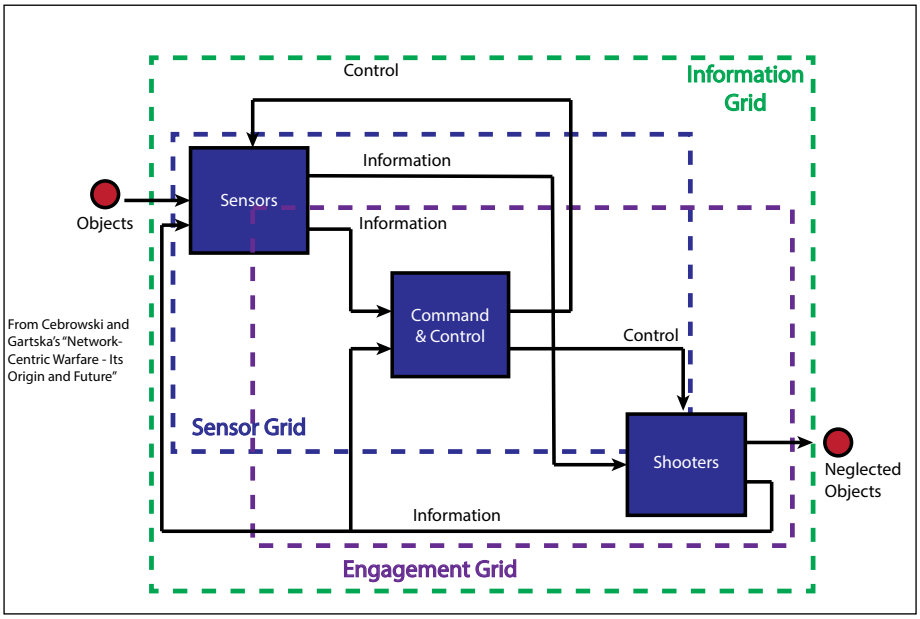

Figure 2.

Achieving a unified, expeditionary, resilient, and interoperable network is equivalent to securing iLOCs. Creating expeditionary capabilities is a familiar problem set: making computers and their supporting equipment Marine and Mother Nature-proof whilst remaining resilient in the face of enemy attempts to deny, degrade, or destroy them. Interoperability requires architecture, protocols, and topologies that are conversant within the Corps, with the Joint Force, the larger Department of Defense, and the rest of the world—especially with our treaty allies and strategic partners. Finally, we must add "a paradigm switch from *information assurance* to *mission assurance*."[23] This shift helps us solve the right part of the fundamental problem of communication for Marines: graceful degradation at the tactical edge.

Graceful degradation at the tactical edge entails mission assurance. Mission assurance means that the necessary iLOC(s) with which to conduct and enable the mission are secured, not all possible circuits along which data can flow. The difference between mission and information assurance is semantically equivalent to the difference between superiority and supremacy. Just like the air and maritime domain, our superiority is contested. Our focus ought to ensure we have the ability to have the capabilities required for the mission *at that time*, but not always. These capabilities must be networked amongst those forward, with the Joint Force, the broader Department of Defense, and the wider world web. iLOCs presents a way to examine how those networks operate and identify where they are vulnerable, like in chokepoints.

We operate in a world where, as the *National Security Strategy of the United States of America* acknowledges, "virtually all modern weapon systems depend upon data derived from scientific and technical intelligence."[24] Yet, the expectation for future operations, like the tactical cloud, rests upon the assumption that we will have robust and secure iLOCs and a surplus of data: Amazon-like logistics requires Google-like IT. Artificial intelligence, considered to be the engine of digital age, requires data—like a fuel—to run.[25] The *Summary of the 2018 Department of Defense Artificial Intelligence Strategy* explains "a *common foundation* of shared data, reusable tools, frameworks and standards, and cloud and edge services" (italics added) is imperative to successful development.[26] These requirements, however, persist after initial the services are developed. To utilize these data-fed weapons requires a path along an iLOC to reach a server for updates, patches, and defensive protections, among others.[27]

To achieve mission assurance requires understanding the network as multiple iLOCs and to consider data and its elements a class of supply. Digital logistics is the process of planning, implementing and controlling the effective and efficient flow of software, hardware, firmware, and related IT services from the point of origin to the point of consumption (along an iLOC) by technology end users. For a squad of Marines using a mesh network this is no different than normal communication requirements. Nor is it particularly different if those Marines use a ROVER to pull full motion video feed from an aircraft. Both can be considered segments of an iLOC.

But when we consider how the combat operations center receives full motion video feed over the network from a remotely piloted aircraft, iLOCs matter. The crucial variable, assuming interoperability, is bandwidth. However, variables concerning security, latency, and message type are also important. This requires infrastructure that leverages at a minimum the Joint network and then its integration with the Marine network. Depending on the architecture, this may even require integration between the DOD network, the Joint network, and then the Marine networks. Full motion video feed from remotely piloted aircraft, for example, is but one capability that requires iLOCs. As we continue to leverage software-defined capabilities, the need to ensure that we have secured the required iLOC is essential. We must have the pathway to reach back to where the data is evaluated, stored, or from which it is derived. Consider, too, accessing the wider web for evaluation of the social media landscape. This requires connections between the Marine, Joint, and DOD networks, and then the ability to access the resources of the Global Informational Grid.

Each integration link is a choke point where bandwidth and logic come to the fore. Multiple pathways are important, like a branch plan is to any course of action. Higher will often receive data with greater resiliency because it directly connects into the Joint or Department of Defense networks. Everyone downstream receives access to these capabili-

ties with the understanding that they pay for access with bandwidth and are beholden to the quality of the network on which they ride. Technologies, like satellite terminals, can only pass so much information so quickly; a commander can have three feeds in standard definition, but one feed in high definition. This is the give and take with iLOCs. By extending an iLOC out into the Joint network, there may be access to additional or difference resources with further possibilities and combinations of sensors and shooters, but there is a price in terms of transiting the chokepoint and the surface area of vulnerability.

Prioritizing which things should pass is essential. These iLOCs, intra (as in the case for the squad), inter (in the Group V RPA case), and extra (for the access to social media, prioritize different capabilities) bandwidth, resiliency, access, and latency. Considerations for these factors require the same diligence of planning as for logistics, because they are as constraining (and amplifying) what would be normal, tangible supplies, such as ammunition, chow, medical supplies, and fuel. Similar to the flow of logistics or the transportation of materials, the flow and transport of information and data must be carefully planned. If we hold to the belief that supply only concerns the tangible—the fuel, the ordnance, and the chow—we miss planning for and managing digital supplies. The is not about sending and receiving email, but about the stream of multiple sensor feeds fused together through artificial-intelligence enabled platforms creating an environment for exceptionally fast kill-chains. Successful data storage, transfer, and utilization are absolutely imperative if we are going to leverage our full networked 21st century combat power against our adversaries. To truly heed Commandant Gen Robert H. Barrow's observation, *amateurs think about tactics, professionals think about logistics*, we need to be sure that the kinds of logistics we are thinking about are all of the resources of our combat power, especially the networking of our information.

Notes

1. Headquarters Marine Corps, *MCDP 4, Logistics*, (Washington, DC: 1997).

2. Carl von Clausewitz, *On War*, trans. J.J. Graham, (New York, NY: Barnes and Noble, 2004).

3. VADM Arthur K. Cebrowski and John J. Gartska, "Network-Centric Warfare—Its Origin and Future,"U.S. Naval Institute, (Online: January 1998), available at https://www.usn.org.

4. David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised), (Washington, DC: DOD C4ISR Cooperative Research Program, 2000).

5. Cory T. Anderson, Dave Blair, Mike Byrnes, Joe Chapa, Amanda Collazzo, Scott Cuomo, Olivia Garard, Ariel M. Schuetz, and Scott VanOort, "Trust, Troops, and Reapers: Getting 'Drone' Research Right' *War on the Rocks*, (Online: April 2018), available at https://warontherocks.com.

6. "Network-Centric Warfare–Its Origin and Future."

7. *MCDP 4, Logistics*.

8. Ibid.

9. Verlyn Klinkenborg, *Several Short Sentences About Writing*, (New York, NY: Alfred A. Knopf, 2012).

10. Headquarters Marine Corps, *MCDP 1*, Warfighting, (Washington, DC: 1997).

11. Robert H. Scales, "Return to Gettysburg: The Fifth Epochal Shift in the Course of War," *War on the Rocks*, (Online: October 2018), available at https://warontherocks.com.

12. *Network Centric Warfare: Developing and Leveraging Information Superiority*.

13. *MCDP 4, Logistics*.

14. Scott Cuomo, Olivia Garard, Jeffrey Cummings, and Noah Spataro, "Not Yet Openly at War, but Still Mostly at Peace: The Marine Corps' Roles and Missions in and Around Key Maritime Terrain," *War on the Rocks*, (Online: October 2018), available at https://warontherocks.com.

15. George Cyrus Thorpe, *Pure Logistics: The Science of War Preparation*, (Kansas City,MO: Franklin Hudson Publishing Co., 1917).

16. *MCDP 4, Logistics*.

17. *On War*.

18. Joint Staff, *Joint Publication 1-02 (JP 1-02), DOD Dictionary of Military and Associated Terms,* (Washington, DC: February 2019). Defines: "line of communications—A route, either land, water, and/or air, that connects an operating military force with a base of operations along which supplies and military forces move. Also called LOC. (*JP 2-01.3*)"

19. For a case that does, see Nicole Starosielski's The Undersea Network. Her work explains how undersea cables, which account for more than 99 percent of intercontinental internet traffic, align with the SLOCs used by the British Empire.

20. C.E. Shannon, "A Mathematical Theory of Communication," *The Bell System Technical Journal*, (New York, NY: American Telephone and Telegraph Company, July/October 1948).

21. Headquarters Marine Corps, *Marine Corps Strategy for Assured Command and Control: Enabling C2 for Tomorrow's Marine Corps, Today*, (Washington, DC: March 2017).

22. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, (Washington, DC: 2018).

23. Jennifer McArdle, *Victory Over and Across Domains: Training for Tomorrow's Battlefields,* (Washington, DC: Center for Strategic and Budgetary Assessments: 2019).

24. Department of Defense, *National Security Strategy of the United States of America*, (Washington, DC: 2017).

25. Michael Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review*, (Online: May 2018), available at: https://tnsr.org/.

26. Department of Defense, S*ummary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*, (Washington, DC, 2018).

27. This includes air-gapping.