The Enemy's Most Dangerous Course of Action

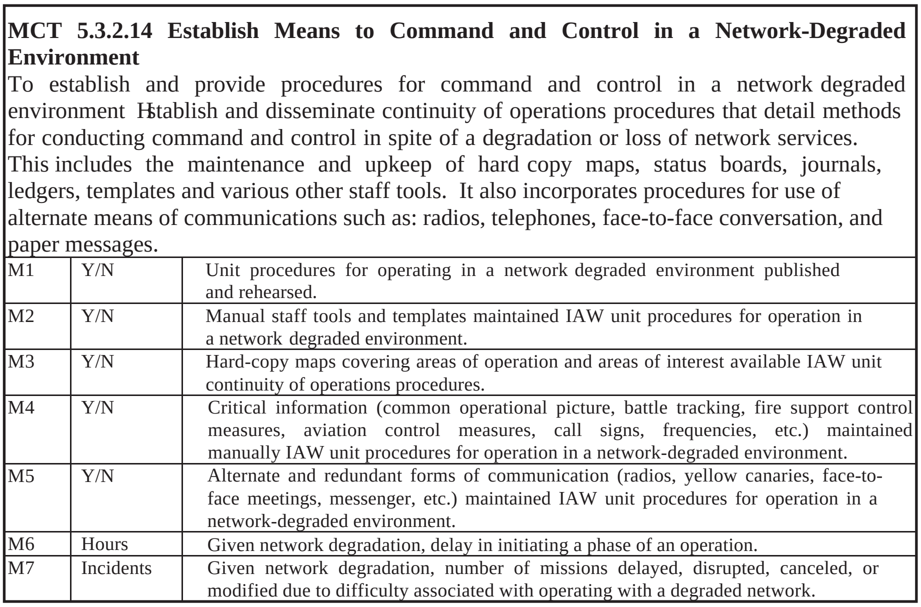
Is the Marine Corps prepared to operate in a network-degraded environment?

by Capt Christopher R. Canter

In the age of net-centric warfare, the Marine Corps has become increasingly reliant on network systems to increase situational awareness, decrease decision-making times, and synergize resource management. The widespread adoption of these systems and the failure to retain institutional knowledge on how to operate without their use have exposed the Marine Corps to vulnerabilities that threaten its ability to operate effectively in future environments. Just as the Marine Corps has recognized the benefits offered by technology and cyberspace, its adversaries have realized that it provides a viable method of attack.

While there is much debate on which of our adversaries possess the capability and willingness to conduct effective cyber operations, less attention has been paid to what effect this would have on our ability to operate. This article is an examination of what would happen if the enemy did in fact possess the ability to deny or significantly degrade our ability to use network-based systems. This article does not delve into the specifics of how an enemy might accomplish such an effect or when they would choose to employ such a tactic. It begins with the assumption that the enemy already has this capability or is actively working to attain it.

By first examining the Marine Corps' reliance on network-based systems and then addressing the argument that the Marine Corps is already prepared for a cyber threat, this article will demonstrate that if the Marine Corps is going to remain relevant in future conflicts, it must formalize the manner in which it trains and evaluates units to operate in a network-degraded environment. By doing so, I hope to raise awareness to this concerning issue and recommend steps that can be taken to correct this deficiency.



MCT 5.3.2.14 Establish Means to Command and Control in a Network-Degraded Environment

To establish and provide procedures for command and control in a network degraded environment Hstablish and disseminate continuity of operations procedures that detail methods for conducting command and control in spite of a degradation or loss of network services. This includes the maintenance and upkeep of hard copy maps, status boards, journals, ledgers, templates and various other staff tools. It also incorporates procedures for use of alternate means of communications such as: radios, telephones, face-to-face conversation, and paper messages.

M1	Y/N	Unit procedures for operating in a network degraded environment published and rehearsed.
M2	Y/N	Manual staff tools and templates maintained IAW unit procedures for operation in a network degraded environment.
M3	Y/N	Hard-copy maps covering areas of operation and areas of interest available IAW unit continuity of operations procedures.
M4	Y/N	Critical information (common operational picture, battle tracking, fire support control measures, aviation control measures, call signs, frequencies, etc.) maintained manually IAW unit procedures for operation in a network-degraded environment.
M5	Y/N	Alternate and redundant forms of communication (radios, yellow canaries, face-to-face meetings, messenger, etc.) maintained IAW unit procedures for operation in a network-degraded environment.
M6	Hours	Given network degradation, delay in initiating a phase of an operation.
M7	Incidents	Given network degradation, number of missions delayed, disrupted, canceled, or modified due to difficulty associated with operating with a degraded network.

Figure 1.

Throughout each warfighting function (maneuver, fires, logistics, intelligence, force protection, and C^2 [command and control]), there exists a significant reliance on network systems to enable forces to gain and maintain the advantage over adversaries. Some warfighting functions are less reliant, but all would experience increased levels of friction and a loss of efficiency if denied the use of network systems. This loss would be intensified because fewer Marines each year have had the opportunity to develop the warfighting skills to operate without network systems.[1]

The Marine Corps' reliance on network systems and lack of preparedness for their eventual loss or degradation

>Capt Canter is the Information Technology Officer, MAGTF Staff Training Program.

***Are Marines prepared to operate in a communications-degraded environment?** (Photo by Cpl Jocelyn Ontiveros.)*

has not gone unnoticed by its enemies. LtGen Daniel O'Donohue, newly appointed Deputy Commandant for Information, once described the perceived critical vulnerability of the U.S. military as cyberspace operations. He later reinforced his statement by saying that the enemy believes it is going to take asymmetric advantage over U.S. forces through its use of cyberspace operations, and it is trying to exploit this vulnerability daily.[2]

When examining reliance on network systems for each warfighting function, several trends exist. First, most functions would be able to fight through the degradation and continue to operate for limited durations.[3] The ability to do this requires up-front planning and coordination and is not sustainable indefinitely. This can be clearly seen in recent MEF and MEB exercises where simulated cyberspace attacks limited network access; impeded capabilities to communicate with higher, adjacent, and subordinate units; and increased the time required to consolidate information, make decisions, and coordinate actions. In these scenarios, the cyberspace attack degraded the unit's ability to C^2 and, in some instances, totally prevented sections from conducting necessary coordination.

It is important to note that each unit eventually overcame the degradation through the use of alternate forms of communications and preplanned transitions to manual staff procedures. While effective in these situations, these were exercises that had included this degradation in their planning. Had this happened in the operational environment today, it is less likely that such a plan would have been established or rehearsed. In this circumstance, functions would still fight through network degradation but would take longer and require greater effort. If the network degradation continued for a prolonged period, the difficulty and delay in coordinating actions would limit operational tempo and responsiveness—making it more difficult to employ maneuver warfare tactics.

Second, some warfighting functions are more severely affected by network degradation. Consider the effect of network degradation on logistics. At the lowest levels, logistical requests and support are coordinated using radios. Immediately following this, however, there is a consolidation of request onto network-based systems. These requirements are then sourced using maintenance and supply management systems.[4] This reliance on network systems for all but the most basic logistic functions represents a serious threat for units faced with operating in a network-degraded environment.

... each unit eventually overcame the degradation ...

For these units, prolonged periods of network degradation would cause significant friction in coordinating large-scale logistics, forecasting demands, and conducting supply chain management.[5] This would reduce the unit's ability to sustain itself, therefore limiting its operational reach. Similar effects would be seen in C^2, intelligence, and, to some extent, force protection. Throughout these functions, there has also been a considerable convergence to network systems. With limited redundant and alternate systems and almost no formal training on how to operate in a network-degraded environment, leaders within these functions must determine how much risk they are willing to accept if their technology were to fail.[6]

Finally, there is a disparity in the perceived effect of network degradation on warfighting functions among leaders. Of those contacted in support of this article, individuals with operational experience beginning in the early 2000s were far more likely to present an optimistic assessment of how each unit would adapt and overcome network degradation. Individuals with operational experience from more recent years offered a bleaker assessment. Having spent their entire career thus far with network systems integrated into all aspects of their duties, younger leaders experienced increased difficulty in trying to operate in a network-degraded environment. Senior leaders, on the other hand, typically displayed a confidence born of their past experiences where they had the opportunity to successfully operate without the ease and efficiency of network systems.

This disparity is important because it highlights a looming threat. While the leadership and experience of senior leaders may currently offset the degree to which a function is negatively impacted because of network degradation, there will eventually be a time in which no leaders are present who have had the opportunity to develop the warfighting skills necessary to operate in a network-degraded environment.[7] If something is not done now to formalize the method in which the Marine Corps trains and evaluates the ability to operate without network systems, the Marine Corps will soon find itself in a position where both leaders and subordinates are forced to relearn hard lessons from the past.

Despite these trends, there are some who believe that the Marine Corps is already prepared for operations in a network-degraded environment. They justify their assertion based on the unprecedented level of attention cyberspace operations are receiving within the Marine Corps and overall Department of Defense.[8] To them, there is little doubt that cyberspace operations are an emerging threat, and they point to recent MEF and MEB exercises that have included simulated cyberspace attacks as proof that the Marine Corps is tackling this head on. Their assessment is further reinforced through the growing number of MAGTF training institutions that have begun to incorporate cyberspace operations into their curriculum.

While all of this is true, it is important to note that none of this has been done to an extent sufficient to truly prepare Marines to operate in a network-degraded environment. For instance, in the case of one recent MEB exercise, the cyberspace scenario ended early to alleviate the network disruptions' effect on the remaining training objectives.[9] This sort of action is not unusual. While most staffs recognize the need to incorporate cyberspace training into their exercises, they do not possess adequate resources or training to prioritize it above other, more defined training objectives.

Similarly, various training institutions, such as the MAGTF Staff Training Program, Marine Corps Tactics and Operations Group, Marine Corps Logistics Operations Group, and Marine Aviation Weapons and Tactics Squadron One, have all met significant difficulty in trying to incorporate cyberspace operations into their curriculum. When speaking to representatives from each institution, all expressed strong desires to incorporate cyberspace operations but were ultimately frustrated in the lack of cyberspace operations tasks within the Marine Corps task list and associated training and readiness standards.[10] These formal requirements are needed to incorporate cyberspace operations to ensure that Marines and their units are being trained appropriately. Despite this frustration, each institution has still attempted to incorporate cyberspace operations. Not having the necessary formal standards, however, has limited their effectiveness in most cases.

The threat of cyberspace attacks and its implications of operating in a degraded network environment are serious issues ...

The threat of cyberspace attacks and its implications of operating in a degraded network environment are serious issues that the Marine Corps must contend with if it is to remain relevant in future operations. Within each warfighting function, there exists some capability to fight through network degradation, but it comes with a significant loss of efficiency and operational tempo. This loss is greater for some warfighting functions, but it can be offset through proper training, rehearsals, and the leadership of those who have had the opportunity to develop the warfighting skills to operate without network systems. As fewer Marines remain who have had the opportunity to develop these skills, it is imperative that the Marine Corps formalizes the manner in which it trains and evaluates operations in a network-degraded environment.

To accomplish this, the Marine Corps must incorporate the requirement to be capable of operating in a network-degraded environment into the Marine Corps task list. This will allow organizations within the Marine Corps to allocate resources and fully incorporate it into their training and exercises. The best and most complete way to do this would be a detailed review of the Marine Corps task list to add, change, or alter tasks within each warfighting function. In an effort to provide a more actionable and timely solution, it is recommended, at a minimum, that the requirement be added as a subtask of MCT 5—Exercise C^2.

Notes

[1] LCDR Steven Bryant, USN, "The Dangers of an Over-Reliance on Technology," (Washington, DC: National Defense University, Joint Forces Staff College, June 2011).

[2] Kevin McCaney, "Lines of Fire: Cyber Operations, Electronic Warfare Will Take the Point in Future Conflicts," *Defense Systems*, (Fort Belvoir, VA: September/October 2015).

[3] Maj Daniel Rosenberg interview with author (14 December 2015); Maj Sean Welch interview with author (1 December 2015); Maj Jeffery Roman interview with author (1 December 2015); Capt Christopher Cichy interview with author (11 January 2016); Capt Caleb Rench interview with author (18 November 2015); Capt Steven Nye interview with author (30 November 2015); Capt Thomas Rigby interview with author (30 November 2015); Maj George Steinfels interview with author (1 December 2015).

[4] Maj Sean Welch interview with author.

[5] Ibid.

[6] "The Dangers of an Over-Reliance on Technology."

[7] Ibid.

[8] "Lines of Fire."

[9] Catherine Norman, William Brobst, and Margaux Hoar, *Achieving MEB Training Objectives: 1st MEB in LSE-14 and Lessons for Future Exercises*, Center for Naval Analyses, (Quantico, VA: Center for Lessons Learned).

[10] LtCol Atiim O. Phillips interview with author (20 October 2015); Maj James W. Bauch email message to author (11 January 2016); Capt Allen V. Pollard email message to author (11 January 2016).