Closing the MAGTF C²/Cyber Gap

The requirement of a C²/Cyber center of excellence
by Maj Paul L. Stokes, USMC(Ret)

Northeast Asia 2020: *The Regimental Landing Team (RLT) Bravo Command Group pulled into position upon completion of the assault of MEB Objective Alpha. LtCol Crusher, the RLT S-3 (Operations), had just begun to brief the remainder of his staff next to his networking on-the-move (NOTM)² staff vehicle (SV) (see Figure 1) when suddenly, the artillery liaison officer looked at his Advanced Field Artillery Tactical Data System and yelled, "Incoming!"*

In an instant, the RLT headquarters' position was plastered with several dozen artillery shells. As the smoke cleared, the S-3 picked himself up and looked around. He gazed at the burning, smoking hulks of a dozen vehicles and the twisted bodies of his Marines. After a couple of deep breaths, he composed himself, barked orders, and assembled what was left of his mobile combat operations center. Fortunately the old man was alive, but the XO, Sergeant Major, S-2 (Intelligence), and S-4 (Logistics) were killed in the barrage, as well as half of the section chiefs.

The RLT's fire support coordination center NOTM SVs were a pile of twisted metal, but fortunately, the S-6 (Communications), Maj Mercury, had the foresight to locate the NOTM point of presence (POP) vehicle about 200 meters away from the RLT headquarters. However, stray shrapnel had damaged the POP's antenna array, reducing its satellite communications bandwidth throughout by 75 percent—severely limiting the RLT's voice, data, and imagery links to the division and its maneuver battalions.

Before he had to ask, the S-3's Operations Chief, MGySgt Ramrod, gave him an assessment of what was left of the RLT C² (command and control) sys-

> ***No single activity in war is more important than command and control. Command and control by itself will not drive home a single attack against an enemy force. It will not destroy a single enemy target. It will not effect [sic] a single emergency resupply. Yet none of these essential warfighting activities, or any others, would be possible without effective command and control.***
>
> ***Without command and control, campaigns, battles, and organized engagements are impossible, military units degenerate into mobs, and the subordination of military force to policy is replaced by random violence. In short, command and control is essential to all military operations and activities.***
>
> ***—MCDP 6, Command and Control*** [1]

tems, and the situation was grim. All he had left was one of the combat operations center's C² personal computers, the fire support coordination center's Common Aviation Command and Control System laptop with a broken screen, the S-4's Common Logistics Command and Control System terminal, a couple of secret Internet router protocol network terminals, a non-secure Internet router protocol network terminal, a dozen voice-over Internet protocol telephones, an assortment of tactical C², intelligence fire support and logistics single channel radio (SCR) nets, and two map boards, and about 29 staff personnel had survived.

To add more fuel to the fire, Maj Mercury reported that enemy cyber attackers had hacked into the RLT secure enclaves and were causing all kinds of mischief to

>**Maj Stokes retired in August 2006 after 31 years of active duty service. A former Gunnery Sergeant and Chief Warrant Officer 3, he has served in a variety of leadership and communications billets from team to theater levels. Maj Stokes has served as the Marine Corps Communication-Electronics School's Deputy Operations Officer, Future Operations/Plans Officer since January 2007.**

the data networks, but the RLT's 06xx cyber Marines were busy countering the threat. This meant that they were back to a push-to-talk SCR, yellow-canary, acetate-overlay, grease-pencil, protractor, green-logbook world, and he needed to take the bull by the horns, repurpose the manpower and material he had at his disposal, and reconstitute the RLT headquarters' core C² capabilities ASAP, before the enemy exploited the fact that the RLT headquarters had become deaf, dumb, and blind.

The MAGTF C²/Cyber Gap

The days of unimpeded global MAGTF communications are over, and the Marine Corps must relearn how to exercise C²/Cyber operations in a denied/degraded environment against a 21st century near-peer competitor. This environment could mean the loss of wideband communications connectivity, which will significantly degrade collaborative planning, targeting, video feeds, and other bandwidth-intensive functions—forcing commanders to resurrect *the will to communicate* by employing narrow-band SCR communications, training their Marines as a team, issuing clear, concise commander's intent/guidance, and allowing subordinates to retain freedom of action.
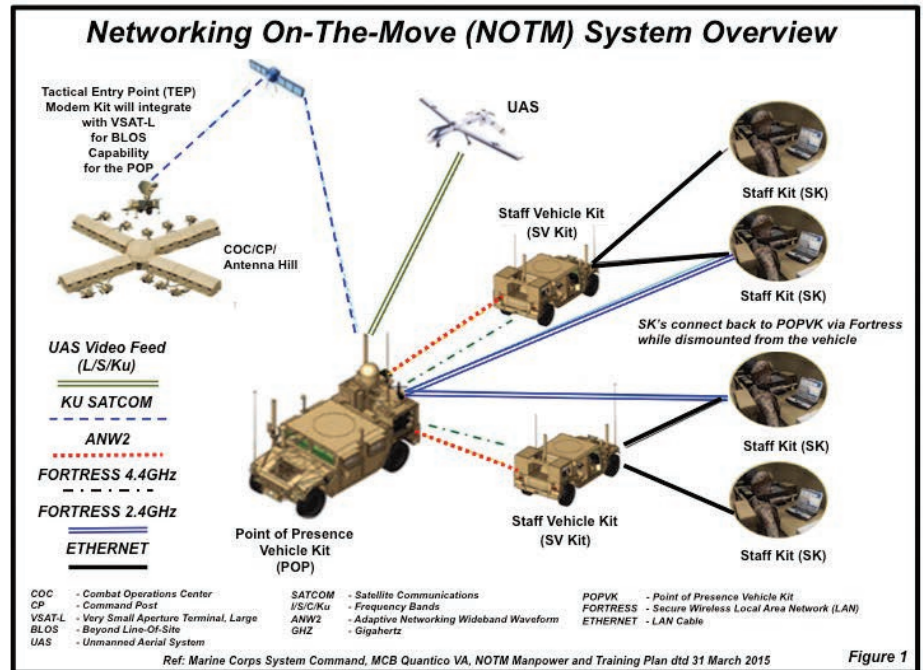

Figure 1. *(Figure provided by author.)*

fectively despite it. We can do this by developing simple, flexible plans; planning for likely contingencies; developing standing operating procedures; and fostering initiative among subordinates.[3]

To some, learning to face and overcome uncertainty is a tall order, especially in this age of instant voice, data, and video

---

Commanders and their staffs must also train to operate in a denied/degraded environment because the decentralization of decision-making authority inherent in this concept mitigates the impact of loss of network connectivity.

Commanders and their staffs must also train to operate in a denied/degraded environment because the decentralization of decision-making authority inherent in this concept mitigates the impact of loss of network connectivity. In essence, we, as leaders of Marines, must re-embrace the basic tenet of uncertainty when it comes to C²;

> because we can never eliminate uncertainty, we must learn to fight ef-

communications. But the simple fact of the matter is all of these services are simply tools that a commander employs to seek out, close with and destroy the enemy—not mythical *deus ex machina* (literally "god machines")[4] that ensure victory. So the question remains: How does a commander foster "a bias for action" throughout his command?[5] And the answer is clear—knowing your Marines and training them as a team in

accordance with combat-proven tactics, techniques, and procedures (TTP).

Closing the MAGTF C²/Cyber Gap

With the Marine Corps engaged in over fifteen consecutive years of combat operations, much has changed in terms of equipment, MOS structure, threats, and new top-down initiatives such as the extension of C² systems to the squad level, cyber operations, and the Marine Corps Enterprise Network (MCEN) and its impact on the tactical edge and digital interoperability. As a result,

> Marines must understand that controlling physical terrain is no longer a sufficient condition for battlefield success; we must also navigate the landscape of knowledge and perception. Operating in the information domain will not only require us to protect our networks but take actions that inform, promote, persuade, coerce, dissuade, convince, compel, deceive, mask, and intimidate.[6]

> We must acquire the offensive capabilities to raise and detect enemy signatures across the spectrum, quickly and accurately assign meaning to what we observe, and rapidly take action to exploit any opportunity. Defensively, our units will need to adapt how they

fight, emphasizing emissions control and other means of signature management to increase their survivability. We will also need deception capabilities that cause an adversary to form inaccurate impressions about our actions and intentions. Further, we will need to improve our counter-intelligence capabilities and social media discipline.[7]

C²/Cyber Training

Presently, the Marine Corps lacks an established organization responsible for integrated C²/Cyber training, which negatively impacts the opposing force's ability to fight and win in a denied/degraded environment against a near-peer competitor.

The Marine Corps could resolve this deficiency by establishing a C²/Cyberspace center of excellence (C²/Cyber COE) that is organized, equipped, and capable of providing realistic training on planning and executing operations in a degraded C4I (intelligence) environment. And the failure to do so will result in needless casualties and, potentially, our ultimate defeat in future conflicts.

C²/Cyber COE Concept of Operations

The C²/Cyber COE would partner with the following organizations in an integrated team led by the Commanding General of the MAGTF Training Center (CG, MAGTF-TC) in order to exemplify their top skills to prepare MAGTF staffs for the challenges of the 21st century battlespace: the Marine Corps Tactics and Operations Group (MCTOG) for their GCE C² operations expertise, the Marine Aviation Weapons & Tactics Squadron One (MAWTS-1) for their aviation C² prowess, the Marine Corps Logistics Operations Group (MCLOG) for their logistics C² acumen, the Expeditionary Warfare Training Groups–Pacific and Atlantic (EWTGPAC and EWTGLANT) for their amphibious/naval integration experience, and the Marine Corps Communication-Electronics School (MCCES) for its cyber/C² technical skills.

The C²/Cyber COE would base its concept of operations/curriculum on the requirements outlined in the *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century,* to include:

- *Integrating the naval force to fight at and from the sea*[8] *through*
  - Defining the role of forward and ready naval forces
  - Defining the MAGTF's role in sea control and power projection
  - Integrating command structures
  - Creating lodgments
  - Understanding littoral operations in a contested environment
  - Employing expeditionary advanced base operations
- *Evolving the MAGTF*[9] *through*
  - MEF-level operations
  - Integrating command, control, and informational tools
  - Unified action
  - Integrating MAGTF-SOF capabilities
  - Understanding the challenges of compositing
  - Training and fighting as distributable forces
  - Exploiting automation
- *Operating with resilience in a contested-network environment*[10] *through*
  - Defining the role of signatures in offense and defense
  - Networking for rapid and precise fires
  - Pushing processing power to the tactical edge
  - Enhancing the concept of intelligence
  - Expeditionary logistics
  - Operational energy
- *Enhancing our ability to maneuver*[11] *through*
  - Naval and littoral maneuver
  - A broader concept of combined arms/information warfare
  - Urban operations and complex terrain
  - Infantry and mobility
  - Light and heavy forces
- *Exploiting the competence of the individual Marine*[12] *through*
  - Seeking high-quality human capital
  - Training and educating Marines for the integrated naval force
  - Developing Marines for complexity
  - Developing leaders at every echelon
  - Cultural learning
  - Emphasizing quality in leadership positions

- Managing talent to improve the return on training/education investment
- *Maintaining a close relationship with*
  - The Deputy Commandant, Plans, Policies, and Operations
  - DC, Aviation
  - DC, CD&I
  - Assistant DC, Information Warfare
  - Director, Command, Control, Communications, and Computers, Headquarters Marine Corps
  - Director, Intelligence
  - DC, Installations and Logistics
  - Operating Forces
  - The Supporting Establishment

Maintaining these relationships would be in order to develop and implement validated C² training and education requirements.

Establishing the C²/Cyber COE

Because its core elements already exist, the C²/Cyber COE wouldn't require new organizations. However, a new set of task-organized command relationships would have to be established via a DC, CD&I charter. These command relationships would provide the CG, MAGTF-TC with the authority he would need as the Director, C²/Cyber COE—to exercise tactical control of the resources from MCTOG, MAWTS-1, MCLOG, MCCES, EWTGPAC, and EWTGLANT in support of his mission to

manage MAGTF Training Program and conduct Service-level MAGTF combined arms training to enhance the combat readiness of the Operating Forces and support the Marine Corps' responsibilities to national security.[13] (See Figure 2.)

CG, Training and Education Command would retain, via CG, Training Command, operational control and administrative control of the C²/Cyber COE maneuver elements. Furthermore, the Training Command would act as the liaison between the MAGTF Staff Training Program (MSTP), the C² COE, and the C²/Cyber COE in order to ensure that all three organizations were synchronized in support of the tenets outlined in the *MOC.*

A Three-Phase Approach

The C²/Cyber COE activation pro-

cess would employ a three-phased approach and would take approximately three years to formally implement.

- *Phase 1—Creation of the C²/Cyber charter/command relationships*

  ▪ DC, CD&I would direct CG, Training Command to stand-up an operational planning team with the task of producing a C²/Cyber COE charter that would establish the COE's mission statement (i.e., to provide realistic training on planning and executing MAGTF operations in a denied/degraded/contested C4I environment), tasks and responsibilities, organization (to include, MAGTF-TC, MCTOG, MAWTS-1, MCLOG, MCCES, EWTGPAC, and EWTGLANT), command relationships, and a plan of action and milestones.

  ▪ CG, MAGTF-TC would review his training exercise and employment plan and explore how the C²/Cyber COE could be used to enhance the MAGTF's ability to conduct C²/Cyber operations in a denied/degraded/contested environment against a near-peer competitor.

- *Phase 2—Integration of C²/Cyber operations into the MAGTF training program*

  ▪ CG, MAGTF-TC, in his role as the Director, C², would oversee the integration of C²/Cyber operations into all aspects of the MAGTF training exercise and employment plan, to include staff training, command post exercises, combined arms, and amphibious exercises.

  ▪ Long-range plans would be developed to link all of the C²/Cyber COE's maneuver elements (i.e., MAGTF-TC, MCTOG, MAWTS-1, MCLOG, MCCES, EWTGPAC, and EWTGLANT) virtually in order to improve MAGTF staff training via existing simulations technology[14] and online training—saving both time and money.

- *Phase 3—Fully Operational Capability*

  ▪ C²/Cyber COE would be fully capable of providing MAGTF C²/Cyber operations training in both virtual and field environments, to include staff training, command post
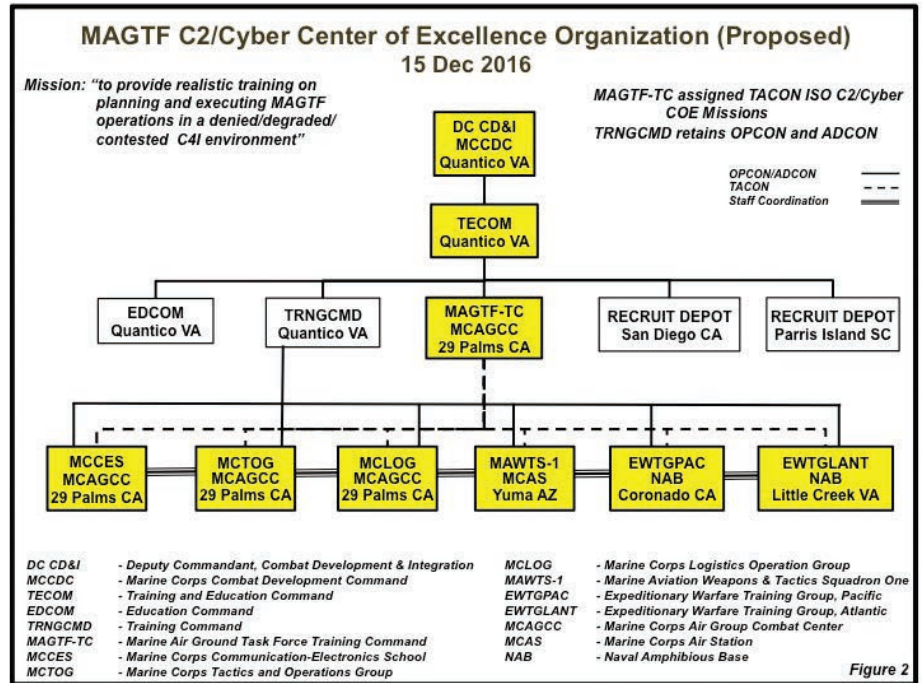

Figure 2. *(Figure provided by author.)*

exercises, and combined arms and amphibious exercises.

Give Our "Young Turks" the Opportunity to "Make it Happen"

In his *FRAGO 01/2016: Advance to Contact,*[15] Gen Robert B. Neller wrote that we must

> grow Information Operations (IO), cyber, and Electronic Warfare (EW) capability at Marine Forces (MARFOR) and Marine Expeditionary Force (MEF) levels to enhance the capabilities of forward deployed forces;

and we must recognize the fact that

> organizing and executing high quality training is a difficult task. It takes time, deliberate thought, and effort. Our approach to training must evolve. It will emphasize the basics: combined arms, competency in the use of our weapons and systems, and expeditionary operations; but it must reemphasize operations in a degraded command, control, communications, computers and intelligence (C4I) environment.

The C²/Cyber COE will exceed the Commandant's C4I training requirements at a minimum cost. Furthermore, it will place all MAGTF C²/Cyber training under a common director—CG, MAGTF-TC—thereby facilitat-

ing the standardization of tactics, techniques, procedures, and doctrine, the synchronization of the overall C²/Cyber and MAGTF training continuum, and the creation of a learning environment that encourages critical thinking and innovation. All that is needed is the willingness and forethought to give our Young Turks the opportunity to make it happen.

Notes

1. Headquarters Marine Corps, *MCDP 6, Command and Control,* (Washington, DC: 4 October 1996).

2. NOTM is employed by selected units across the MAGTF down to the infantry company level and will be employed across the range of military operations. NOTM is a C² system that provides commanders and their staffs with an improved, continuous, and reliable operational capability for uninterrupted access to the common operational picture for digital C². NOTM allows commanders and their staffs to rapidly coordinate with subordinate or neighboring units and provides reachback to command elements using digital C² applications and tools while at the halt and on the move. The NOTM system provides the capability to link and extend defense information systems network services (i.e., secret Internet router protocol network

terminals and non-secure Internet router protocol network terminals). Additionally, NOTM is enhanced with full-motion video capabilities integrated into the NOTM network architecture. NOTM is a capability comprised of six principal end items—C^2 NOTM POP HMMWV/M-ATV variant; C^2 NOTM POP AAV variant; Network Management System, NOTM SV Kit HMMWV/M-ATV variant; Network Management System, NOTM SV Kit AAV variant; C^2 System, NOTM Staff Kit; and Modem Communications, NOTM Tactical Entry Point Communications Modem Kit—that are used to achieve the C^2 functional extension of combat operations center networks, services, and workstations to the commander and his staff when displaced from the static combat operations center. Ref: Marine Corps System Command, MCB Quantico, VA, "NOTM Manpower and Training Plan," 31 March 2015.

3. Headquarters Marine Corps, *MCDP 1, Warfighting,* (Washington, DC: 20 June 1997).

4. LtCol Richard Leino, "MAGTF C^2 and the Deus Ex Machina," *Marine Corps Gazette,*

(Quantico, VA: August 2008), provides an excellent treatise on the pitfalls of relying solely upon technology to resolve the challenges of C^2.

5. This section of the article was extracted from: Maj Paul L. Stokes, "The Will to Communicate," *Marine Corps Gazette,* (Quantico, VA: September 2016).

6. Headquarters Marine Corps, *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, (Washington, DC: September 2016).

7. Ibid.

8. Ibid.

9. Ibid.

10. Ibid.

11. Ibid.

12. Ibid.

13. Marine Air-Ground Task Force Training Command's mission statement, available at www.29palms.marines.mil.

14. The U.S. Army has extensive experience in employing simulations to train their staffs, to include the Corps Battle Simulation and Battle Command Training Program. Each major U.S. Army base has a simulation center that can be linked via commercial communications providers to other Army bases, allowing them to conduct a wide range of training from battalion to corps levels. The Marine Corps should learn from this experience and link together the C^2/ Cyber COE maneuver elements in a similar manner. See http://www.globalsecurity.org.

15. Gen Robert B. Neller, *FRAGO 01/2016: Advance to Contact*, (Washington, DC: 19 January 2016).

>*Editor's note: Deus ex machina doesn't "literally" translate to "god machines" but rather "god out of (or from) the machine."*