Marines trust Harris IT Services to unify their enterprise for cost-effective mission success

Harris IT Services designs, builds, and supports assured communications® solutions that enable government and commercial customers to meet their missions, on time and within budget. Leveraging Harris Corporation's long legacy of deep engineering expertise, IT Services is uniquely positioned to deliver end-to-end communications and IT solutions with speed and flexibility.

That's why our customers – including those in defense, intelligence, homeland security, civil, and commercial markets – rely on us to solve their difficult IT and communications challenges, as well as maintain those solutions 24/7/365.

HARRIS assuredcommunications®

Visit us online at www.itservices.harris.com

RF Communications • Government Communications Systems • Broadcast Communications • IT Services

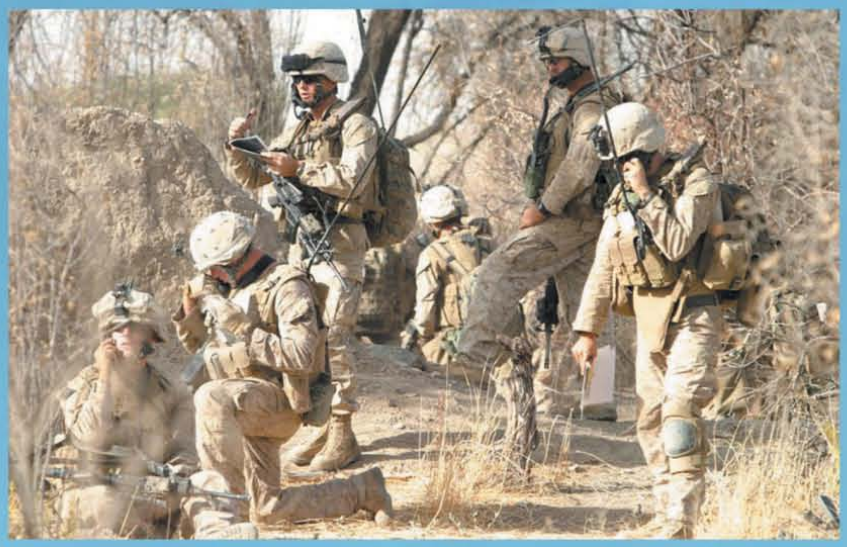
SIGNAL Magazine's USMC IT Focus

SIGNAL Magazine has teamed with the AFCEA Quantico-Potomac Chapter to produce this series of articles that focus on Marine Corps information technology (IT) organizations and training. We hope you enjoy this special IT overview of the Marine Corps.

Within these articles are details on:

- C4/CIO Vision
- MCCDC's Role and Requirements Evolution
- Open Architecture
- Commercial IT
- Information Technology Challenge
- Information Assurance Rules
- Marine Corps Requirements Process
- Marine Corps Acquisition Cycle
- Network Operations and Security Center
- MARFORCOM G-6
- MCCES
- Tactical Systems Support
- Tomorrow's Information Technology Leaders
- Warfighting Lab Capabilities
- Service Catalog
- Quantico-Potomac Chapter Support to the Warfighter

SIGNAL Magazine and the Quantico-Potomac Chapter wish to express a special appreciation to Harris Corporation for the level of sponsorship provided for the USMC IT Focus supplement.



USMC IT Focus

APRIL 2010

AFCEA

A SUPPLEMENT TO *SIGNAL* MAGAZINE

U.S. Marine Corps photo by Lance Cpl. Drew Barker

Marines trust Harris Falcon® radios to help secure the battlefield. Trust our land mobile radios and critical communications networks to secure Marines and their families at home.

From P25 base communications systems with emergency dispatch to mission-critical enterprise networks, Harris helps military and civilian emergency responders communicate reliably, quickly, and effectively. Communications you can depend on—on the battlefield and at home.

To learn how our proven IP-based communications solutions protect Marine bases, call 1-888-711-7295, ext. 3975, or email BaseSecurity@harris.com.

HARRIS® *assuredcommunications®* *www.harris.com*
RF Communications • Government Communications Systems • Broadcast Communications

AFCEA Vision and Introduction to U.S. Marine Corps IT Day

On behalf of AFCEA International, welcome to the Quantico Chapter's Marine Corps IT Day. *SIGNAL* Magazine has teamed with the Quantico-Potomac Chapter and the U.S. Marine Corps to develop a series of articles that introduce Marine information technology (IT) organizations and training. We hope you enjoy the articles that support this special IT overview of the Marine Corps.

As you know, AFCEA's primary mission is to provide an ethical forum for dialogue among military, government, industry and academia on issues of critical importance to the command, control, communications, computers and intelligence (C^4I) and IT communities in the global security environment. IT days like this one, run by our chapters, are a critical part of that dialogue. Through this forum, both government and industry will provide an update on the state of C^4I and IT program planning and execution; budget and policy issues; and future direction for the Marine Corps and the joint and coalition environments. Senior government leaders, program executive officers and program managers will talk about priorities, needs for input and upcoming opportunities for industry support. Industry leaders will provide the state of the market as it pertains to the Marine Corps and will have the opportunity to provide feedback and ask questions of the government participants.

Clearly, you all could have this dialogue through a series of one-on-one meetings with the principals, but nowhere will you find a venue to provide a more comprehensive look at the Marine Corps C^4I/IT program structure and receive the synergy of the perspectives of all the participants, both government and industry. The power of that collective conversation will allow the government participants to leave with a better understanding of the current and emerging capabilities of industry and will allow industry participants to leave with a better understanding of the current and future needs of the government in this space.

Thanks to the Quantico-Potomac Chapter for organizing and presenting this forum to the leadership of the Marine Corps C^4I community and to industry for your participation. I trust you all will walk away with better understanding and collaboration on these critical C^4I programs.

Kent R. Schneider
President and Chief Executive Officer
AFCEA International

AFCEA INTERNATIONAL

4400 Fair Lakes Court, Fairfax, VA 22033 • 703-631-6100

President and Publisher ..... Kent Schneider
Vice President, Publications
Associate Publisher ..... Beverly P. Mowery
Senior Director, Publications
Editor in Chief ..... Robert K. Ackerman
Managing Editor ..... Jim Sweeney
Associate Editor ..... Katie Packard
Art Director ..... Chris D'Elia

AFCEA ONLINE

AFCEA Home - www.afcea.org
***SIGNAL* Online** - www.afcea.org/signal
***SIGNAL* Blog** - www.afcea.org/signal/signalscape
SIGNAL Connections - www.afcea.org/signal/connections

QUANTICO-POTOMAC CHAPTER

Chapter President - Mike Warlick
571-437-0685 or president@afcea-qp.org
Chapter Secretary/Membership - Steve Gaudreau
540-658-1146 ext. 312 or secretary@afcea-qp.org

U.S. Marine Corps C4/CIO Vision

Future warfare will take place in increasingly complex and uncertain environments against state and nonstate adversaries that employ conventional and irregular capabilities, terrorist acts and criminal disorder. This hybrid form of war defines an era where information beats kinetics, and it illustrates the imperative that Marines must fight as effectively in the information environment as in any other domain.

Winning in the information environment drives our need to dynamically harness relevant and timely data, information and knowledge resident with people and technology to accomplish our mission. Developing networks, communications and information technologies (IT) that help knowledgeable people communicate and collaborate through secure and trusted networks enhances organizational agility and competitive advantage.

By Maj. Gen. George J. Allen, USMC

Whether we facilitate information sharing or knowledge creation to support conventional, irregular or hybrid operations, homeland defense or international/domestic disaster response, we must develop networks, communications and IT capabilities that respond dynamically to the varied needs of our Marines and civilian workers, regardless of mission, mission partner or global location.

To accomplish this, it is imperative that we develop interoperable communications and information-sharing technologies and implement supporting policies to maximize effective collaboration across and outside our organization. Interoperability with mission partners must enable the Marine Corps to lead multinational and joint operations and to enable interagency activities. We must evolve the Marine Corps Enterprise Network (MCEN) to fully integrate tactical and supporting networks, improve bandwidth to the tactical edge and provide dispersed users with mobile secure solutions. Additionally, we must develop reachback solutions that leverage our garrison infrastructure to support dispersed users that operate in austere and challenging environments.

Our garrison infrastructure also must meet Marine Corps business requirements and processes for manning, training and equipping the force. We cannot overstate the importance of our networks, as they deliver the information we need to perform our legislated role. Because we value information as a strategic asset, we will ensure that we implement an enhanced information assurance (IA) posture—one that protects operational and personal information while simultaneously enables organizational agility. This posture will adopt a model that blends the exercise of centralized command and decentralized control with defense in-depth practices and technologies.

Finally, all of this must be done under the imperative of "green IT." The Marine Corps takes this requirement seriously and fully intends to comply with federal, U.S. Defense Department (DOD) and Department of the Navy (DON) policies and regulations regarding energy. From a green IT perspective, we can significantly reduce the Corps' energy consumption by adopting new practices and technologies and by sensibly consolidating IT capabilities and services with our sister military services.

Marine Corps IT Goals

Marine Corps investments in IT support the National Defense Strategy, the National Military Strategy, DON and Marine Corps warfighting and business process priorities. The following represent the Marine Corps' IT goals:

- Develop responsive, agile, integrated and defendable networks,
- Enable a network-centric Marine Corps by developing a collaborative and data-rich information-sharing environment,
- Provide responsive, agile and relevant support to expeditionary, garrisoned and mobile users,
- Provide secure networks, IT systems, data and critical information infrastructure,
- Provide sustainable and recoverable systems,
- Implement effective governance processes,
- Ensure green IT,
- And ensure improved IT investment decision making and a cost-effective IT environment.

Marine Corps Enterprise Objectives

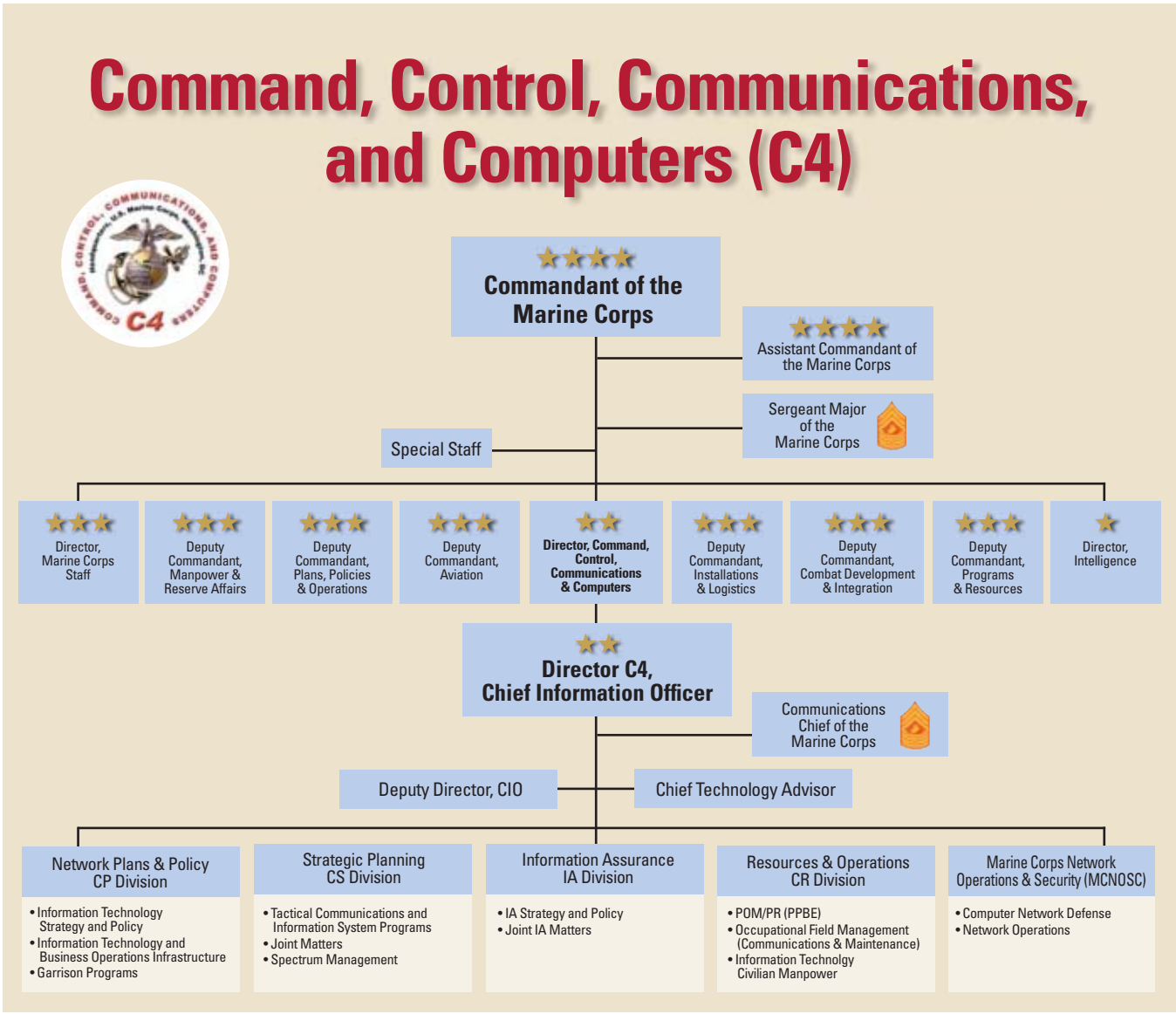
The objectives listed below represent specific actions that must be achieved in order to accomplish specific goals. These objectives will impact investment decisions, programs, concepts of operations and processes.

- Build networks that interoperate with expeditionary forces, garrisoned organizations, other services, federal and DOD agencies, coalitions and nongovernmental organizations;
- Enable commanders to increase the speed of their decision cycle and operate at an ever-increasing tempo;
- Integrate Marines, command and control platforms and

weapons into a networked, network-centric distributed combat force;
- Implement the Joint Concept of Operations for Global Information Grid (GIG) network operations to manage, defend and provision content on the network;
- Establish a service-oriented architecture strategy and implementation plan to create a more agile, cost-effective and secure Marine Corps IT infrastructure;
- Implement a data strategy that makes data visible, accessible and understandable to all authorized users and eliminates redundant data sources;
- Employ IA as a central component of all networks, applications and data systems;
- Implement a green IT strategy that supports the Marine Corps Expeditionary Energy Office objectives; applies environmental practices, energy efficiency and waste reduction; and is in compliance with and meets appropriate directives;
- Improve IT asset visibility and network situational awareness;
- Align and synchronize training with emerging technology to ensure the Marine Corps work force is capable of maintaining and defending increasingly complex and sophisticated IT systems and networks;
- And establish common platforms to maintain and optimize network functions and resources.

Accomplishing the above will help Marines succeed in complex, distributed or garrison environments and will assist the U.S. Marine Corps in fulfilling its role as the nation's premier expeditionary force in readiness.

Maj. Gen. George J. Allen, USMC, is the director for Command, Control, Communications and Computers (C4), and the deputy Department of the Navy chief information officer for the U.S. Marine Corps.



The MCCDC's Role and Requirements Evolution

By Lt. Gen. George J. Flynn, USMC

The U.S. Marine Corps develops warfighting capabilities and requirements through the Expeditionary Force Development System (EFDS). EFDS is a four-phased process that is executed cyclically and is synchronized with the Planning, Programming, Budgeting and Execution System and the Defense Acquisition System. EFDS guides the identification, development and integration of warfighting and associated support and infrastructure capabilities for the Marine Air Ground Task Force (MAGTF). The commanding general for the Marine Corps Combat Development Command is dual-hatted as the deputy commandant for Combat Development and Integration (CD&I). The deputy commandant leads the execution of this process and collaborates throughout with numerous stakeholders across Headquarters Marines Corps, the operating forces and the supporting establishment.

Each iteration of EFDS begins with a capabilities-based assessment (CBA), a deliberate and collaborative analytical process designed to identify current and future required capabilities and tasks to execute Marine Corps operating and enabling concepts. CBA guidance is provided by pertinent vision or strategy documents published by the commandant of the Marine Corps, complemented by guidance from the three-star Marine Corps leadership, such as the Marine Requirements Oversight Council (MROC). Additionally, warfighting capability needs are determined by analyzing the Marine Corps concepts against Concepts of Operations and defense-planning scenarios selected by the MROC. Each capability need that is identified has standards established so that it is understood what must be achieved to meet operational and tactical requirements depicted in the selected scenarios. The required capabilities identified during each cycle of EFDS are captured and published in the MAGTF Capability List (MCL). Once the MCL is developed, further analysis is conducted to identify the capability gaps, shortfalls and excesses that exist in the Marine Corps' present force structure capabilities. Capability gaps are identified by assessing actual performance capabilities against the standards. The results of this analysis are compiled, prioritized and published in the MAGTF Gap List (MGL). Both the MCL and the MGL are provided to the MROC for review and approval.

Once the MCL and MGL are completed, a solutions analysis is conducted. The solutions analysis identifies strategies for eliminating capability gaps. It also features a solution-planning directive that details how the Marine Corps will implement the preferred solutions as well as a MAGTF requirements list that prioritizes existing programs and new initiatives for consideration during the next program objective memorandum cycle. The first part of the solutions analysis is conducted using Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) working groups to identify potential solutions. These groups are comprised of subject matter experts across Headquarters Marine Corps, the operating forces and the supporting establishment. The groups' recommended solutions are published in a solution planning directive that the deputy commandant for CD&I develops and submits to the MROC for approval. The directive provides specific tasks to organizations in order to mitigate or eliminate the capability gap. The solutions analysis concludes with publication of the MAGTF requirements list, an integrated, prioritized list of materiel and nonmateriel solutions (including new initiatives and existing programs) for consideration during the next program objective memorandum development process. The MROC is the approval authority for the requirements list, which serves as an initial requirements baseline and is subject to continuous refinement.

The results of the solutions analysis then are integrated into the resourcing and programming phase of the EFDS, called program development. The materiel solutions identified in the solutions analysis phase compete for resourcing during this phase. Criteria consistent with guidance provided during the EFDS's CBA phase are developed and applied against each materiel solution. The materiel solutions are evaluated against the criteria—both new initiatives and programs of record—and the materiel solutions are prioritized and prepared for submission as the Warfighting Investment Program Evaluation Board (WIPEB) input to the Marine Corps program objective memorandum. The program evaluation boards, which are designated by the deputy commandant for Programs and Resources, the program objective memorandum working group and the program review board (a one-star review board) evaluate the MRL and recommend to the MROC programs and initiatives to be funded in the upcoming program objective memo-

randum. The program development phase concludes when the WIPEB recommendations are integrated with other investment recommendations and forwarded to the MROC as the tentative program memorandum objective.

The fourth and final EFDS phase is capabilities implementation and transition, which includes all aspects of delivering coherent and fully integrated warfighting capabilities to the operating forces. Phase Four continues through the employment and monitoring of capability solutions identified in the solutions analysis.

Concurrent with the EFDS process, the capability integration officers assigned to the deputy commandant for CD&I are responsible for preparing and producing the Joint Capabilities Integration and Development System (JCIDS)-compliant capabilities documentation. Like the EFDS, this is a CD&I-led collaborative process that uses many of the subject matter experts who participated in the CBA, solutions analysis and program development efforts. These experts support the CD&I's integrated product teams, which are responsible for preparing JCIDS documentation required by the chairman of the Joint Chiefs of Staff and the acquisition community. These include DOTMLPF change requests, initial capability documents, capability development documents and capability production documents.

As is the case with every POM, difficult requirement development decisions are inevitable and expected. By employing an analytical process that is guided by the Marine Corps senior leadership, and considering all stakeholder perspectives, EFDS accumulates the data and analysis required to effectively prioritize requirements and establishes an informed framework where smart tradeoffs can be made.

Lt. Gen. George J. Flynn, USMC, is the deputy commandant for Combat Development and Integration, Marine Corps Combat Development Command.

Find out more about the Marine Corps Combat Development Command by visiting: **https://www.mccdc.usmc.mil/**.

Open Architecture and a Joint Environment

By Brig. Gen. Michael M. Brogan, USMC
Commander, Marine Corps Systems Command

As the Marine Corps shifts its focus to Afghanistan with its formidable terrain and austere infrastructure, it is imperative that we integrate our resources with those of the other military services and coalition partners so everyone can bring full force to bear on the battlefield. This requires help from our industry partners. At the same time, we must have the flexibility to respond to a resilient enemy without the hindrances of proprietary restrictions. An open architecture system affords us the broadest opportunity in our area of operations to converge systems and heighten our overall situational awareness.

We need to be architecture-driven so we can reduce the total number of disparate systems to those that are actually required. Similar to how commercial televisions accept any DVD player, open architecture allows each individual component, much of which is non-developmental and commercially available, to "plug and play" within the architecture and does not tie us to proprietary systems. Through open software standards we can achieve corresponding "plug and play" capabilities with our software applications, and only minor integration will be required to adapt or modify these applications to suit the warfighter requirement. In our Marine Corps Systems Command (MCSC) vision, the government will own the data rights so that we can more rapidly execute updates and upgrades without beholding to an individual contractor. This lets the command look after the best interests of the American taxpayer.

An example of this is what the Program Manager, Common Aviation Command and Control System (CAC2S) is doing with his Aviation Command and Control Suite. He has a single operational view and integrated architecture that the various functions "plug" into. Other programs, such as the Combat Operations Cen-

Combat Operations Center (outside view)


Operations Trailer

ter (COC) and Marine Air Command and Control System (MACCS) are then allowed to become contributors to facilitate CAC2S.

For example, to make the COC "plug and play," the COC leverages modular design and design disclosure. The COC implements the five principles of Modular Open Systems Approach (MOSA):

- Establish an enabling environment
- Employ modular system design
- Design to key commercial standard interfaces; these include ST Fiber; High-Speed Serial (530 to serial); CAT 5e (RJ45); and Coaxial (BNC)
- Use open standards
- Certify for conformance (allocated and functional baseline configuration audits)

The COC employs reusable application software. There is open competition for best-of-breed candidates, reviewed by subject matter expert peers to include CAC2S. Mandated design disclosure and documentation is available to all sources, and this is non-negotiable. This approach leverages Interoperable Joint Warfighting Applications and Secure Information Exchange using common services.

COC Prime Contract and Integrated Product Teams (IPT) have adopted an Enterprise Management Model that encourages collaboration among government and industry teams. As such, CAC2S is an invited member of the COC Systems Engineering IPT. COC Configuration and Risk Management Plans include CAC2S representation as members of the Configuration Control Board (CCB) and Risk Management Board (RMB). This ensures system compatibility is maintained during COC sustainment and modernization.

The MACCS Communication Information System (CIS) provides an open architecture system to be used as the basis for the CAC2S Communications Subsystem (CS). The CIS provides an air support control system to give commanders with the aviation combat element of the Marine Air Ground Task Force the capability to plan, implement and adjust air support operations effectively. Like the COC, the CIS was developed using commercial off-the-shelf and standard radios and interfaces.

Using this open architecture, we cannot afford to field a solution from one vendor and then be tied to that vendor in perpetuity.

The other area we are most concerned with is creating interoperability between our Command and Control Situational Awareness (C2/SA) capabilities and those of the United States Army. As directed by the Joint Requirements Oversight Council, Marine Corps Systems Command and the Army's Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA ALT) the work is a first step to converging C2/SA capabilities across the entire joint force.

We initially charted a path by conducting a joint Army-Marine Corps study using the MITRE Corporation to identify those systems and protocols that will lead to interoperability on the battlefield and eliminate stovepipes.

This convergence effort is essential because the Marine Corps, due to its expeditionary nature, routinely operates within a joint environment. Working closely or even cross attaching units with the U.S. Army has become commonplace in Iraq and Afghanistan. Success in these operations depends in part on the ability to exchange information between the services. While this might sound trivial in the age of BlackBerrys and Internet gaming, establishing interoperability between military organizations in a foreign country that does not have a telecommunications infrastructure can be difficult.

The challenge for the two Services is much like getting a Playstation 3 (PS3) video game to work with an X-Box 360 system. While the two systems have similar functions, players tend to have their preference as to which system works best for them. To make them interoperable, the gaming stations (hardware), connections (communications) and security (firewalls) must all be aligned to work together or the players cannot exchange information.

Much like the PS3 and X-Box example, the Army and Marine Corps have been fielding different systems for many years tailored to support their unique approaches to combat operations. To create interoperability, the two services have chartered a systems engineering effort to work this challenge with their program managers and industry partners.

This effort, known as Army and Marine Corps C2/SA Convergence, is evaluating the way the two services' battle command applications exchange tactical data. To make them interoperable, we also must evaluate and standardize the language used by the applications (data models); how the networks address and route (network operations), how they are protected (information assurance), as well as the communications and the technical standards used in the exchange. This is an extensive effort and requires the integration of multiple programs of record as well as fielded systems developed by different vendors. The teamwork and cooperation between our industry partners and the Systems Command is the only way we can achieve this goal.

We walk a fine line as we draw from the best industry has to offer and still maintain our independence to reach our goals free from restrictions. Our vision — our essential support to the forward deployed lance corporal — requires the best effort from us and all our service and industry partners.

Brig. Gen. Michael M. Brogan, USMC, is commander of the Marine Corps Systems Command.

Col. Peter C. Reddy, USMC, Erik J. Gardner and Jeffery D. Wilson of the Marine Corps Systems Command contributed to this article.

Find out more about the Marine Corps Systems Command by visiting: **https://www.marcorsyscom.usmc.mil/.**

Adopting Commercial IT

USMC IT Requirements and Capability Vision

The Marines Corps is following Headquarters Marine Corps Command, Control, Communications and Computer's (C4's) integrated communications strategy, a comprehensive vision, strategy and planning document intended to unify and synchronize the efforts of the Marine Corps information technology (IT) community to meet the needs of the warfighter and those who support the warfighter. This document represents interim strategic direction for integrated communications and networking through 2015. The USMC continues to evolve and improve its IT and information management capabilities, including horizontal information fusion across functional areas, network and information superiority at the tactical level, information assurance and security, collaboration and IT asset visibility.

By Dr. John Burrow

Marine Corps IT Constraints and Considerations

Marines rely on IT systems to coordinate their actions and activities across the range of military operations. As we continue to evolve the Marine Corps' IT capability, we must consider many factors to adapt the Marine Corps' current IT environment to meet Marines' needs. These factors include bandwidth in austere environments, diminishing resources and conditions imposed by diverse tactical environments. Gaps and challenges we face in adapting our current environment include ensuring high availability, disaster recovery and continuity of operations across the range of military operations; encryption of sensitive and unclassified data, whether in motion or at rest; dispersed IT environment, unique IT systems and one-to-one interfaces; dispersed data and information, resulting in access constraints; dispersed application service desks; and redundancy in data and Web sites, many with tailored solutions/implementations.

USMC IT Direction

The Marines are migrating to network-centric operations in concert with the overall U.S. Defense Department transformation strategy. As part of the overall migration strategy, the Marine Corps Systems Command emphasizes areas that include state-of-the-art technology, interoperability; responsiveness in fielding capability; product agnostic; security for network operations and network defense while enabling exploitation by Marine Air Ground Task Force commanders and users; reducing IT portfolio total cost of ownership while improving IT portfolio management/governance; and implementing the Defense Department network-centric data strategy of making data visible, accessible, understandable, trusted and interoperable.

A more open, modular architecture of hardware, software, applications, data and services is key to our migration strategy. We believe an open architecture allows for increased competition, affordable and rapid technology upgrades, and reduced life-cycle costs; it allows helps us avoid technology obsolescence.

One example of using an open architecture approach to meet Marine Corps mission requirements is the Marine Corps Enterprise IT Services (MCEITS) program. A key component of the Marine Corps implementation of Global Information Grid 2.0 strategic plans and network-centric warfare, the MCEITS hardware and software infrastructure is being built in Kansas City, Missouri, using a commercial off-the-shelf design that embraces all the above areas of emphasis. When completed, the MCEITS solution will share many features advertised by commercial data centers, although our specific implementation and configuration will be unique.

The Marine Corps continues to leverage and implement commercial IT technologies to meet mission requirements, and our needs and objectives have much in common with industry. In fact, our common solution space far exceeds the differences we have, but differences do exist. For this reason, our commercial off-the-shelf acquisition strategies often require us to make hard choices on "state of the shelf" versus "state of the art."

Benefits, Limitations and Risks of Commercial IT

Although the basic functionality of our USMC applications often mirrors their commercial counterparts and respective configurations, differences exist in security, mission (for example, business versus national defense), and command and control implementations. The Defense Department has specific security implementations to protect its enterprise that must change with the threat. Sometimes changes to a security solution in our enterprise adversely impacts other commercial solutions.

The Defense Department—including the Marine Corps—seeks standards-based solutions. Most industry solutions are standards based; however, many solutions tailor these standards to improve product capabilities, sometimes adding complexity and introducing interoperability problems when applied in a military or government environment. Industry can be slow to converge on a standard, sometimes allowing multiple competing standards to coexist for a given functionality, which may create challenges across the government and military domains. While the Defense Department is a major customer in the commercial IT marketplace, history has shown that the department does not always have the leverage necessary to influence the commercial IT space when compared to market sectors. Therefore, commercial business strategies can be at odds with customers who strive to remain product agnos-

continued on page 23

Civilian Marines and the Information Technology Challenge

Not that many years ago, all communications and information technology (IT) were done exclusively by Marines or contractors due the unique training required to conduct network operations. As our civilian Marines became more engrained in daily operations, they took on more roles in IT, especially in circumstances when a close parallel to commercial operations could be seen, such as with base telephone. Today, our civilian Marines of the Information Technology Management Community of Interest (ITM COI) are involved in every facet of Marine Corps IT.

By James P. Craft

As of October 2006, there were 1,212 civilian Marines in the ITM COI, the majority of them in the 2210 information technology specialist occupational series, with 154 civilian Marines in IT-related engineering occupational series. As of February 2010, there were 1,784 civilian Marines in the ITM COI and 186 in other IT-related fields. This is a relatively small number compared to other military services but still demonstrates a 44 percent increase in only three years. The number may well grow another 40 percent in the next three years.

What is driving that growth? The answer has many components, including the desire by Marine Corps senior leadership to put more Marines into the fight; the current administration's desire to "in-source" contractor positions; the ongoing work to move outsourced networks to government-owned, government-operated and contractor-supported networks; the growth in IT complexity; and the number of supported systems.

The growth is not only in numbers but also in the professionalization and skills of the civilian Marines who shape, support and operate our networks and communications. In the future, we will focus more on creating a continual improving, lifetime learning culture through professional development and the selection of meaningful work objectives and experiences. The development will be in five areas: leadership; technical competencies (hard skills); professional competencies (soft skills); Marine Corps enculturation; and preparations for members of a "civilian expeditionary work force." As a way to better meet the mission, life balance also will be emphasized, following the models outlined in such classic business books as *The Seven Habits of Highly Effective People* and *The Power of Full Engagement.*

Despite the growth in numbers, our IT organizations remain extremely lean. For example, Marine Corps bases often support ratios of 1 IT professional for more than 150 user accounts. Although a 1-to-50 ratio would be considered an efficient operation in the private sector, that is not the case for us. The Marine Corps routinely reviews its task organizations (T/O) to ensure the force meets its operational demands. Similarly, the Marine Corps is seeking the right number of civilian Marines in IT and communications. To find this number, a classic "troop to task" analysis is ongoing. The Marine Corps is continually refining its work force structure and aligning it to standardized Information Technology Service Management (ITSM) processes that are being implemented across the Marine Corps. Every ITSM process also is being analyzed to identify automated tools that can make execution of the process both effective and efficient—increasing capabilities but keeping us lean.

The ITM COI is a primary means for shaping our work force. We are the only Marine Corps COI with a full-time COI manager who helps take the ITM COI to the next level. Our base and regional COI leaders now have been appointed in writing by their supervisors. The COI passes vital information to its members and works collaboratively on improving the COI through regular town hall meetings, workshops and conferences. The new ITM COI portal is vibrant. We are making strategic investments in training and looking for new ways to advance the education of the COI, such as leveraging AFCEA courses and various federal distance-learning opportunities.

The Marine Corps ITM COI has made phenomenal progress in the last few years, and that progress is acknowledged outside of the Marine Corps. Our civilian Marines are performing at the highest of levels, both individually and as team members. This year our chief technology adviser and COI manager were recognized as Federal 100 winners, selected by *Federal Computer Week* as one of the top 100 Federal IT employees. Numerous other ITM COI members have received awards from the Department of the Navy Chief Information Officer, AFCEA and other organizations.

Civilian Marines are involved in and are improving IT at every level. We are helping to aggressively transition to the Next Generation Enterprise Network. Various external inspections are showing some of the best results in the U.S. Defense Department in areas such as security and network operations. The ITM COI is being innovative, cutting costs, maximizing efficiency and increasing effectiveness. Most importantly, our Marines are being supported, both in the fight and at home.

In a few short years, the scope of responsibility and impact of the ITM COI on the Marine Corps' daily operations has expanded beyond what is normally associated with most government civilians. The ITM COI's impact on the warfighter and business operations is significant. Around the world, men and women are proving that they understand the tradition they must uphold when they bear the title "civilian Marine."

James P. Craft is the deputy director for Command, Control, Communications and Computers (C4), and deputy chief information officer of the Marine Corps.

Rules of the Road for Information Assurance

When we first learned to drive, the importance of following the rules of the road was impressed on us. Some of these rules were to always signal your intent when turning or changing lanes. Always follow the posted speed limit. Come to a full and complete stop while looking both directions before continuing. Being in the military stationed overseas, we had to learn new rules. Much of what we learned as a youth applied, but we had to learn the local nuances. Not only did we have to learn the meaning of the signs, but we also had to learn how to drive on "the wrong side of the road" in Okinawa or on the Autobahn in Germany. One important rule of the road in Germany is to stay to the right unless you are passing. The importance of learning the rules in both cases was to be safe and not to be a risk to others. This same approach—following the rules of the road—applies to our information assurance (IA) or cybersecurity efforts today.

By Ray Letteer

Operating an information system or a network enclave in the U.S. Defense Department (DOD) means following some very specific rules of the road. DOD Directive 8500.01E and DOD Instruction 8500.02 as well as Chairman, Joint Chiefs of Staff Instruction 6510.01E provide many of those basic rules of the road. Both the directive and the instructions point to following the Secure Technical Implementation Guides, or STIGs, which are a set of specific security settings and configurations established to provide a level of assurance that the systems design and operation of DOD system- and IA-enabled devices will ensure the following: that DOD information is kept confidential, that it is not subject to unauthorized alteration or change, and that it is available for use when needed. The Federal Desktop Core Configuration (FDCC)—which is an Office of Management and Budget mandate—provides an additional set of rules that require all federal agencies to standardize the configuration of approximately 300 settings on each of their computers that use Microsoft Windows XP and Windows Vista. The reason for this standardization is to strengthen federal information technology security by reducing opportunities for adversaries to access and exploit government computer systems.

While the DOD rules establish a common safety and security baseline across the agency, services and DOD organizations sometimes add specific requirements or additional security nuances to these rules based on network configuration, mission and risk. As the Marine Corps Designated Accrediting Authority, we have some flexibility in what specific STIGs are implemented, but it is always based upon the risk to Marine Corps information and the subsequent impact on the Marine Corps mission. We have reviewed a significant number of security tests and identified settings that ensure an achievable and balanced security profile for our systems. We also are finalizing a Marine Corps enterprise desktop solution in coordination with the Marine Corps Systems Command to meet the FDCC settings.

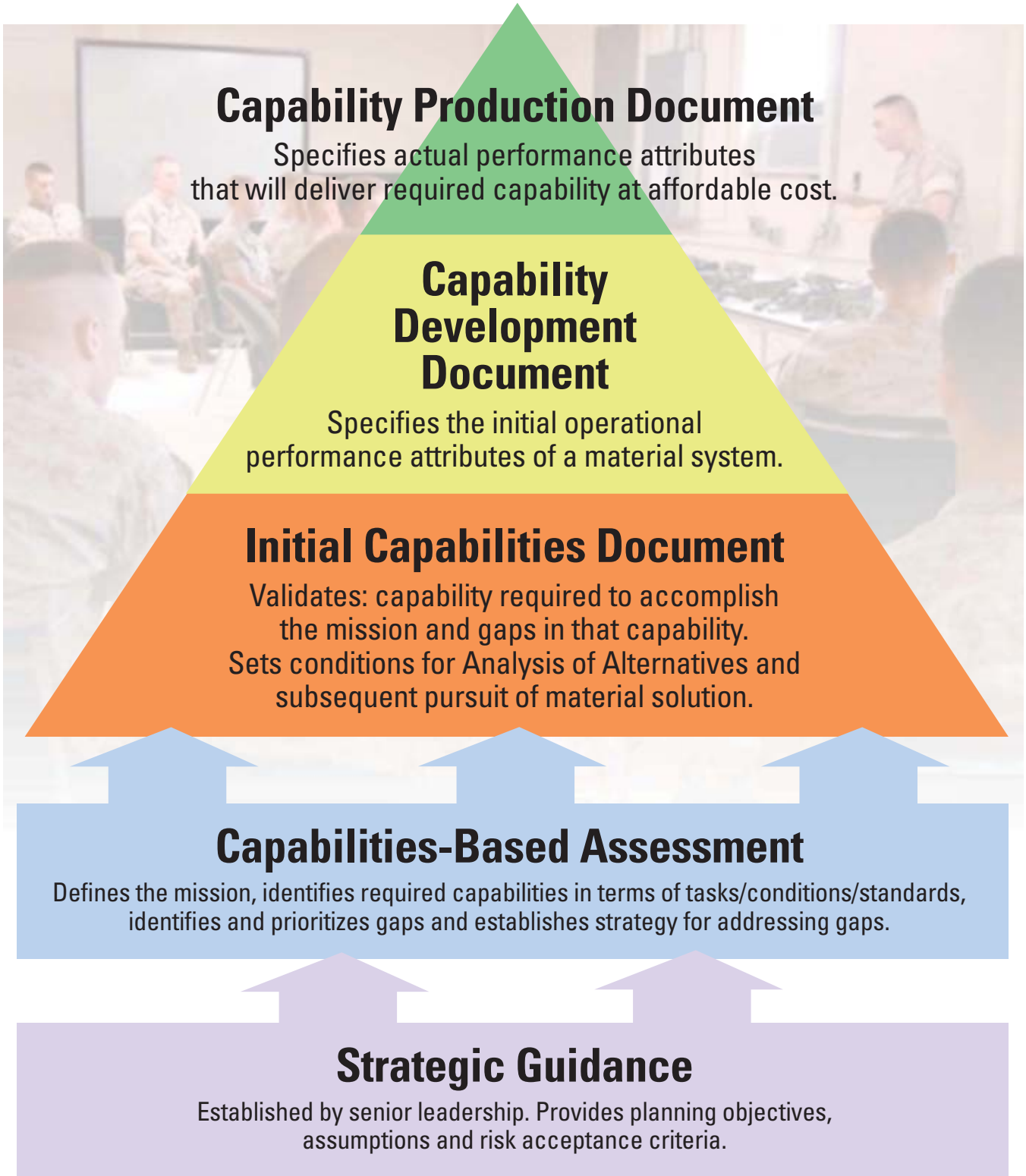
To assure a secure and stable IA profile for our systems, it is imperative that both industry and government have a clear idea upfront about what IA rules apply. Government's responsibility is to provide those expectations early in the acquisition process, preferably while the design stage still is being discussed. In this way, the vendor or developer knows exactly what is expected and can provide it early, thus avoiding significant re-engineering costs later. It also is the government's responsibility to ensure that any deviation from the established security controls is kept to the absolute minimum. The specific security controls presently are identified in DOD Instruction 8500.01, Enclosure E, as well as the National Institute of Standards and Technology Special Publication 800-53A. We also have related security controls with the intelligence community in Committee on National Security Systems Instruction 1253. The government is working actively toward a convergence of security controls to reduce the confusion and cost to industry.

On the other hand, industry's responsibility is to design and develop products that are secure, safe and stable, following the security requirements defined in the design stage. It no longer is prudent to take a commercial product, design the proposed operational capability and then add the security on afterward. The result is that often the security blocks unsafe actions coded in the capability, and the only recourse seems to be to ask for a waiver or other relief in the security requirement. Starting with a secured operating system and using trusted compliers and coding with secured components built in allows for the development of a capability that can run securely from initial design, on a safe platform, and can be protected as future security patches are applied without adversely affecting function. This is the "building IA in" rather than "adding it on later" concept.

As with driving on the highway, when we all follow the rules of the road, we can get to our destinations safely. The same applies in our IA and cybersecurity efforts. With both government and industry following the rules together, we can ensure a safe and secure information system environment for our warfighters, who depend upon these systems to accomplish their missions.

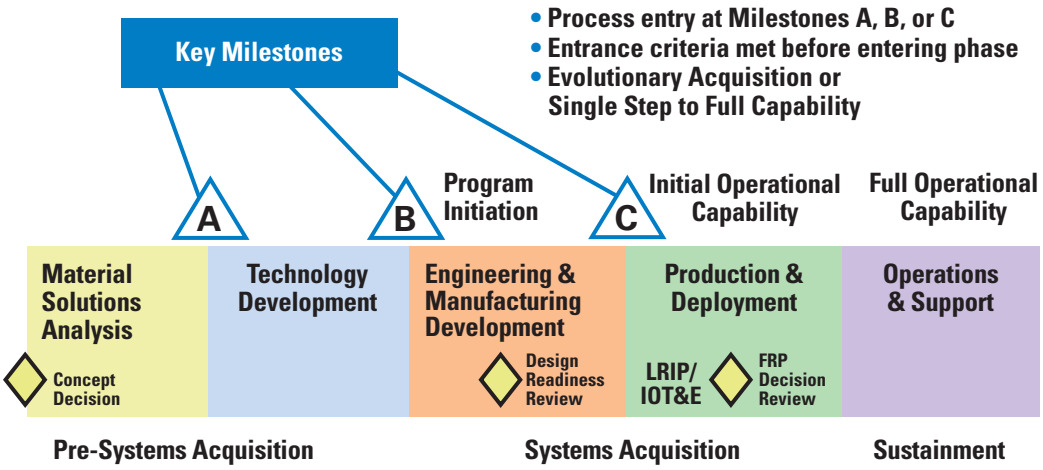
Ray A. Letteer is the director for the information assurance division, Command, Control, Communications and Computers (C^4) Department, U.S. Marine Corps.

Marine Corps Requirement Process



Marine Corps Acquisition Cycle

Acquisition Timeline



DOD Acquisition Process Flow Chart:
https://acc.dau.mil/IFC/index.htm

ASN RDA website:
https://acquisition.navy.mil/rda/home/aquisition_one_source/organizational_points_of_contact_by_subject

MCSC website for Doing Business with MARCORSYSCOM:
http://marcorsyscom.usmc.mil/vendor

Overview of the Marine Corps Network Operations and Security Center

The Marine Corps Network Operations and Security Center (MCNOSC) is under the operational control of the commander, U.S. Strategic Command, who has delegated operational control to the commander, Joint Task Force – Global Network Operations (JTF-GNO). The Director, Command, Control, Communications and Computers has administrative control. The MCNOSC is organized similar to an infantry battalion with six sections: command information management, S-2, S-3, S-4, S-5 and S-6.

By Col. Robert A. Gearhart, USMC

The MCNOSC's mission is to direct global network operations and defense of the Marine Corps Enterprise Network (MCEN) and provide technical leadership to facilitate seamless information exchange in support of Marine and Joint Forces operating worldwide. MCNOSC is the Corps' nucleus for enterprise data network services, network support to deploying forces, and technical development of network-enabled IT solutions. The MCNOSC is responsible for operations involving all aspects of the Marine Corps Enterprise Network. The MCNOSC's tasks include:

- Operate and manage the information transport infrastructure
- Operate and manage the information flow.
- Operate and manage the information and network defense systems.
- Collect and share Global Information Grid (GIG) situational awareness (SA) for MCEN and view GIG SA information from other sources.
- Command and control the MCEN to report, coordinate, and direct actions in response to operational incidents.
- Provide deployed support to ensure Marine Forces can effectively utilize GIG resources.
- Provide technical leadership to ensure Marine Corps and joint capabilities leverage new technologies to our warfighting advantage.

MCNOSC Operations Center personnel monitor MCEN operations around the clock through an array of strategically positioned sensors to ensure the availability and security of the network. The commanding officer of MCNOSC is responsible for directing daily operations to accomplish the JTF-GNO assigned mission of defending the MCEN against cyber attack. This includes preventative actions, attack detection, and incident response to the rapidly increasing number of threats to Marine Corps use of cyberspace. The following core capabilities enable the MCNOSC to present and maintain a responsive, robust, and formidable network operations and defense posture for the Marine Corps Enterprise Network (MCEN):

- Marine Computer Emergency Response Team (MARCERT)
- Integrated Intelligence and Law Enforcement
- Marine Corps Information Assurance Red Team
- Vulnerability Management Team (VMT)
- Direct technical control of non-NMCI Enterprise Services such as firewalls, Active Directory, Global Directory Management
- On-site network support for deploying units
- Enterprise PKI, DMS, and Mainframe operations and technical support
- Technical Design for Enterprise Solutions
- NMCI Vendor Network Watch Team
- Enterprise class operations center and service desk

MCNOSC command relationships are projected to be adjusted in the near future in accordance with Full Operational Capability of USCYBERCOMMAND and MARFORCYBER on October 1, 2010. Under a future OPCON relationship to MARFORCYBER, the MCNOSC will continue to conduct network and defensive cyberspace operations in support of Marine Corps and national requirements.

Col. Robert A. Gearhart, USMC, is the commanding officer of the Marine Corps Network Operations and Security Center.

USS IWO JIMA Landing Force Operations Center (LFOC) upgrades.

Marine Forces Command G-6

By Col. Ken Gill, USMC

The Commandant of the Marine Corps, Gen. James T. Conway, and Lt. Gen. Richard F. Natonski, Commander of Marine Corps Forces Command (MARFORCOM), operate under this dictum: "Our Marines and Sailors in combat are our Number One Priority." This remains the guidepost for MARFORCOM G-6.

MARFORCOM G-6's purpose is to enable the commander with command and control (C2) capabilities through the application of information systems. In addition to the C2 of subordinate units and installations, MARFORCOM G-6 facilitates the operational readiness of Operational C4 units and Marine Corps Bases Atlantic through proactive interaction with Headquarters, U.S. Marine Corps and U.S. Joint Forces Command.

Nested with the commandant's combat priority and our stated purpose, we have identified three areas to remain focused upon:

- NGEN (Next Generation Enterprise Network), which is the follow-on to the NMCI (Navy/Marine Corps Intranet) and the RNOSC (Regional Network Operations and Security Center), our regional management of the Marine Corps Enterprise Network (MCEN). This endeavor is fundamental to our work with Marine Corps Installations East (MCIEAST) and the foundation for our support to the warfighter.
- Marine Expeditionary Unit (MEU) C4 support and Amphibious engagement with Second Fleet and Fleet Forces Command.
- Equipment sourcing for deploying forces and reset of equipment for CONUS units training requirements.

To meet the challenges of accomplishing our purpose and focus areas – the commandant's priority – and because of our pending OPCON requirements in support of the MCEN and transition to NGEN, we have organized MARFORCOM G-6 into two divisions that are similar to what one would find in a deployed G-6: Current and Future Operations. Additionally, the MARFORCOM G-6 construct supports the Director, C4/CIO of the Marine Corps' concept of "Operationalizing the Network."

We execute all tasks from either Current or Future Operations, with 12 officers, 41 enlisted, and 11 civilians. In a broad view, Current Operations is focused on the current operational status of our networks and as required, their prioritized repair, while Future Operations executes our Force G-6 planning responsibilities.

Current Operations, led by Lt. Col. Cindy Rosen, includes the RNOSC, MCEN Operations, Information Assurance/Computer Network Defense and our headquarters' Support/Help Desk section.

As the East Coast is the lead for the Marine Corps effort on transitioning to NGEN, MARFORCOM G-6 Current Operations is preparing by establishing the RNOSC (IOC on November 1, 2009), detailed working relationships with MCIEAST at Camp Lejeune, the Marine Corps Network Operations and Security Center (MCNOSC) in Quantico, and the OPCON and reporting requirements for the NIPRNET and SIPRNET of (in addition to MARFORCOM) Marine Corps Forces South, Marine Corps Forces Europe, Marine Corps Forces Africa, and our associated CONUS bases, posts and stations and all their C4 services – such as information assurance, e-mail services, message services, Internet access, portal access, file services, print services, BlackBerrys, VTC, phone, and data storage). Similar to any commander on the battlefield, the Marine Corps C4 community is focused on

developing a comprehensive (network) common operational picture that delivers the right information to the right level at the right time. This includes leveraging commercial industry best practices like IT services management and adapting those practices to meet a Marine Corps operational construct. A successful Current Operations division enables our staff to operate and the commander to command, and this is their endstate.

Future Operations, led by Lt. Col. Danny Hurd, supports C4 Plans, Amphibious C4, Spectrum, Circuit Management, EKMS, Joint Force Sourcing/Planning, Marine Requirements Board (MRB), Marine Requirements Operational Council (MROC) as well as all MARFOR level Budget Support.

Future Operations truly has feet in two canoes. One is the engagement against our nation's enemies and how we source Marine C4 units, equipment and personnel in support of that fight. In this "canoe" they engage proactively to ensure personnel and communication capabilities are available to deploy and support the Marine Corps assigned mssions. The other foot is pointed forward and they provide guidance and input to HQMC and JFCOM on Marine Corps future policy and requirements as they pertain to C4 and C2.

While engaged in this challenge, Future Operations is a key component of supporting the commandant's direction to continue a "forward naval presence." In addition to the traditional Navy/Marine Corps collaboration challenges, fiscal restraints and limited training time due to worldwide commitments makes amphibious communication planning even more difficult. However, the Marine Corps is returning to greater amphibious training and amphibious C4 capability must be available. Future Operations assists in this enterprise through constant engagement with Second Fleet, the MEUs, HQMC, Marine Corps Systems Command, other MARFORS, as well as Fleet Forces Command.

In summary, our focus remains on the Marines and sailors in the current fight and all they may need ashore and afloat – while ensuring we have a robust supporting establishment network to enable MARFORCOM and our Major Subordinate Commands the C2 capabilities they require.

Col. Ken Gill, USMC, is the G-6 Marine Forces Command.

Find out more about the Marine Forces Command by visiting: **www.marines.mil/unit/marforcom/pages/welcome.aspx**

Marine Forces Command G6 Measures of Effectiveness

- Advance the cause to defeat our nation's enemies.
- Pursue the safety and welfare of our Marines.
- Improve yourself and the G-6.
- Sustain excellence in your performance and never be satisfied.
- Seek Responsibility; Be a leader, and have a bias for action.

How the MCCES Prepares Network Marines

By Maj. Paul L. Stokes, USMC (Ret.)
Maj. Criston W. Cox, USMC and
Master Gunnery Sgt. Anthony L. Russell, USMC

The Challenge

Since the mid-1990s, network-centric warfare has been the driving force behind the design, procurement and fielding of command and control (C^2) systems throughout the U.S. Defense Department in general and the U.S. Marine Corps in particular. In many respects, these efforts have been successful to the point that there are more radios, computers, telephones and satellite systems in a Marine infantry company in 2009 than there were in a Marine infantry battalion during the operation Iraqi Freedom "March to Baghdad" in 2003. However, this success has come at a price—in the form of increased cross-training requirements for our enlisted communications Marines (06XX and 28XX). A combat-effective communications Marine must be able to send/receive digital messages via a tactical radio; operate a tactical voice over Internet protocol telephone system; and set up, connect and operate a laptop computer in a combat operation center as part of a command, control, communications and computers (C^4) network—in other words, these Marines need to do it all, regardless of whether it is voice, video or data.

In order to ensure that our communications-electronics Marines are trained and ready for current and future C^4 systems and service requirements, the Marine Corps Communications-Electronics School (MCCES), Twentynine Palms, California, and its three regional communication training centers (CTCs) at Camp Pendleton, California, Camp Lejeune, North Carolina, and Okinawa, Japan, are

Network-Centric Warfare: "What do I know, who else needs to know it, have I told them, if not—what is the fastest way to get it to them? What format do they need it in, and when they get it—will they understand it?"

—Marine Corps Communication-Electronics School (MCCES), Campaign Plan Fiscal Year 2009

Radios are just part of the Marines' communications training.

integrating network-centric or "Network Marine" training throughout the 06XX and 28XX training continuums.

In addition to these efforts, MCCES has assisted the Marine Corps Forces Special Operations Command (MARSOC) to validate this concept through its MARSOC Network Operators Course, which trains Marines in all three disciplines: radio, data and wire. Although the course is tailored to the MARSOC mission, it has proven that Marines can be trained in more than one discipline while retaining a primary focus on one discipline. To complement this effort, the MCCES CTCs have also developed courses for Incidental Radio Operators and Communication NCOs in order to "bridge the gap" between the formal schools and the OPFOR.

The Network Marine Transformation Begins

In 2008, based on OPFOR Combat After Action Reports (AARs), direct input from HQMC C4 and new equipment fieldings, MCCES overhauled both its Tactical Data System Operator (0651) and Field Wire Switching (0612) courses. These actions have resulted in the creation of two new courses: The Data Systems Technician Course (DSTC) and the Telephone Switch Installer Maintainer Course (TSIMC). Both of these stress IP-based operations as well as how to integrate voice, data and video systems over a single tactical network. In addition, MCCES is expanding its training syllabus to include the core concepts of networking, helpdesk functions, routing, switching and Windows.

For those Marines whom are unable to come to MCCES, the CTCs provide training in a variety of disciplines such as managing a Domain Name Server (DNS), Active Directory, IP Security (IPSEC), Dynamic Multipoint Virtual Private Networks (VPN), and Everything over IP (EoIP) systems. Furthermore, the CTCs are certified Pearson Vue & Prometric test facilities, as well as Certified Cisco and Microsoft Train-

ing Academies, providing Marines no-cost CCNA, CCNP, and MCSA training/certification. They also are the primary vehicle that the USMC uses to achieve DOD 8570.1 Information Assurance Workforce compliancy by providing Comptia A Plus, Network Plus, and Security Plus certification, as well as ISC^2 CISSP training/vouchers.

What Challenges Lie Ahead?

Retraining the Existing 06XX and 28XX Structure
This task is the heart of the Network Marine evolution and requires commanders' direct involvement, resident courses, and distance learning courses to lead the way forward. MCCES has already taken the lead on addressing this challenge by:

Creating a Senior Courses Training Section (SCTS) to consolidate activities and improved cross-training between the Wire Chief Course (0619), Radio Chief Course (0629), Data Chief Course (0659) and Comm Chief Course (0699) via a "core" Network Marine curriculum.

Revamping of the 0621 Course to provide our Field Radio Operators training on a variety of new tactical radios being used by the OPFOR (i.e., PRC-117, PRC-150, VRC-110 and PRC-153) as well IP networking.

Beginning the Development of a Systems Chief Course for 06XX SSgts to bridge the gap between Entry and Senior-Level MOSs by giving radio, wire and data staff sergeants the systems integration training they need in order to support Network operations to include architecture design, Information Assurance requirements, and Defense Information Systems Agency (DISA) procedures for establishing Defense Information System Network (DISN) services in a deployed environment.

Marine Corps Tactical Systems Support Activity: Leading the Way to Support the Warfighter

Marine Corps Tactical Systems Support Activity (MCTSSA) is a tenant command aboard Marine Corps Base, Camp Pendleton, California. Its parent command is the Marine Corps Systems Command, located in Quantico, Virginia. MCTSSA's mission is to provide Marine Air Ground Task Force (MAGTF) and joint command, control, communications, computers and intelligence (C^{4}I) system and system-of-systems technical expertise and support throughout all phases of the acquisition life cycle. As part of its day-to-day operations, MCTSSA serves as the Marine Corps' only dedicated facility to provide system-of-system testing (SoST) of tactical systems.

By Col. Alan M. Pratt, USMC

MCTSSA is home to a highly technical work force that features a nearly equal distribution of 400 military and civilian personnel. The majority of the Marine officers serving at MCTSSA are recent graduates of the Naval Postgraduate School, and they possess degrees in a variety of technical disciplines. Similarly, the majority of enlisted Marines work in technical specialties. The civilian work force is diverse and boasts a strong contingent of electrical and computer engineers and telecommunications specialists as well as a significant number of computer scientists. This combination of military and civilian professionals brings together a unique combination of technical and operational experience, which enhances the command's ability to support tactical C^{4}I systems. MCTSSA's primary customers include the Marine Corps Systems Command, the Program Executive Officer Land Systems (PEO LS) and the Marine Corps Operating Forces. Given a focus of effort spanning the entire acquisition life cycle, MCTSSA plays a key role in the development, testing, fielding, and sustainment of tactical C^4 systems and technology.

MCTSSA provides technical support such as programmatic, engineering, fielding and sustainment of tactical C^4 systems that are developed or maintained by Marine Corps Systems Command product groups (PGs), with a majority of the effort aligned with PG-10 Information Systems and Infrastructure, PG-11 MAGTF C^2, Weapons and Sensors Develop-

Designing a CTC Communication Planners' Course for SSgt through captain. This course covers the planning/integration of a variety of systems (i.e., SWAN, TSM, GMF, LMST, etc.) and in addition, is meant to fill "the expertise gap" that was created by the rapid fielding of these and many other pieces of IT equipment.

The Way Ahead

MCCES is in the process of restructuring its Communication Training Continuum and replacing it with a Network Marine focus. We have the tools, skills, knowledge and HQMC C4 guidance "to make it happen." In addition, with continued support of HQMC, the training establishment and the operational forces, this initiative will succeed.

After all, our Marines deserve nothing less.

Maj. Criston W. Cox, USMC, has been at the Marine Corps Communications-Eletrocnics School (MCCES) since July 2009, where he is the director for the MCCES Warfighter Support Branch, which includes the communication training centers and the distance-learning program. He also is the MCCES director for communications.

Master Gunnery Sgt. Anthony L. Russell, USMC, has been a Marine communicator for 18 years. Since June 2009, he has served as the MCCES battalion operations chief.

Maj. Paul L. Stokes, USMC (Ret.), spent 31 years in active-duty service. He has served as the deputy director for operations at the MCCES since January 2007.

For more information about the Marine Corps Communications-Electronics School, visit the Web site at https://www.29palms.usmc.mil/tenants/mcces/mcceshome.asp.

ment and Integration, PG-12 Communications, Intelligence and Networking Systems, and the PEO LS.

MCTSSA's location is a benefit to its test and evaluation efforts. Its close proximity to the I Marine Expeditionary Force, West Coast naval warfare centers and several defense contracting companies provides an attractive venue for program managers who require system testing. MCTSSA's breadth of testing activities include functional-based testing, system-level verification and validation, network utilization and load testing, SoST and operational assessments.

In terms of physical resources, MCTSSA is home to the C4I Systems Integration Facility (SIF). The SIF is a scalable, fully instrumented test bed that contains a representative sample of fielded tactical systems, network connectivity and communications equipment. It constitutes a command and control environment that is representative of a notional Marine expeditionary force or any lower-level command. The SIF provides a dynamic and operationally relevant environment in which systems can be tested at a single echelon or across multiple echelons. The SIF test environment often is extended to other services through the extensive connectivity available to MCTSSA test personnel. MCTSSA possesses secret Internet protocol router network, nonsecure Internet protocol router network, secure defense research and engineering network, Defense Information System Network-Leading Edge Services, satellite communications, T-1 and microwave links that afford connections when and where they are needed to perform the requisite testing. Designated as the Marine Corps' joint participating test unit, MCTSSA participates regularly as the Marine Corps node in Joint Interoperability Test Command-sponsored interoperability tests, DOD interoperability communications exercises and the joint users interoperability communications exercises.

At the MCTSSA, Marine and civilian personnel work on systems integration testing.

MCTSSA evaluates equipment both in the lab and under operational conditions.

MCTSSA also is the test organization responsible for the continued development and execution of the Marine Corps C4I Capability Certification Test (MC3T). The MC3T initiative is focused on system-of-systems testing. The overall approach consists of the identification, testing and certification of systems that collectively provide MAGTF warfighting capabilities. The MC3T uses a

The MCTSSA serves as a test bed for satellite communications equipment.

persistent, instrumented and controlled SIF environment featuring operationally relevant test threads as a basis to certify system-specific warfighting capabilities. This approach allows for new systems to be integrated into a known and certified environment and subsequently tested to evaluate different aspects of a system's interoperability. Additionally, this approach reduces some of the complexities inherent in SoST. The MC3T is intended to better ensure that deployed MAGTF systems will be fully interoperable and capable of performing intended system functions. This testing and certification effort eliminates the need for warfighters to serve as ad hoc systems integrators and instead allows them to focus on the battle at hand.

MCTSSA testing and technical support efforts have provided simultaneous benefit both to the Marine Corps' acquisition community and to forward-deployed operating forces. Testing efforts have ranged from on-the-move communications testing in support of the Mobile Modular Command and Control (M2C2) vehicle and detailed assessments of new Joint Tactical Common Operational Picture workstation software to the MC3T efforts discussed above. The breadth of technical support provided daily to the operating forces includes a 24-hour C^4 help desk to support fielded applications and forward-deployed contact teams providing technical assistance as well as to offer an ongoing role in providing assistance for the support wide area, a recently fielded capability that significantly increases a Marine unit's ability to receive network services on today's battlefields. Collectively, the Marines and civilians of the MCTSSA strive to provide tactical value through technical excellence. Whether engaged in the development and testing of new systems or the support of fielded MAGTF capabilities, the MCTSSA team stands ready.

Col. Alan M. Pratt, USMC, is the commanding officer, Marine Corps Tactical Systems Support Activity (MCTSSA), Camp Pendleton, California.

Building Tomorrow's Information Technology Leaders

For the Communications School, Training and Education Command, Quantico, Virginia, this vision serves to reinforce its commitment to providing professional and technical training in tactical communications systems in order to ensure that all commanders have the ability to exercise command and control throughout the operating environment.

Although still located in Edson Hall, the school is a markedly different place from the days when lieutenants trained to be "2502s"—the precursor to the Military Occupational Specialty (MOS) 0602 (communications officer). Most notably, the programs of instruction (POI) for the Basic Communications Officer Course (BCOC), Advanced Communications Officer Course (ACOC) and Warrant Officer Communications Course (WCC) recently have undergone thorough updates in both content and structure in order to better reflect the leadership skills and technical training necessary for the newly minted lieutenants and warrant officers and the more seasoned captains and majors to effectively operate in a complex information technology (IT) environment in support of a variety of Marine Air Ground Task Force (MAGTF) operations. These officers must understand the equipment and their command's concept of operations and information requirements—only then can the S-6/communications officer plan, install, operate and maintain (PIOM) an integrated voice, data and video communications network.

By Lt. Col. Robert C. Wright, USMC

The field of communications' student educational process begins with intense preparation by the Communications School instructing staff, which collectively has years of opera-

"We are moving…to a network-centric and service-oriented architecture so the warfighters and those who support them can more easily access the tools and data they need, regardless of location or operating workstation…"

—Maj. Gen. George J. Allen, USMC, director, HQMC C4/CIO for the Marine Corps Integrated Communications Strategy (ICS) Overview, Nov. 20, 2008

tional experience in operations Enduring Freedom and Iraqi Freedom. Additionally, the staff follows a continuing education program that maximizes industry standard certifications that the Marine Corps has embraced within the communications community. The baseline programs that the staff implemented included but is not limited to: Security+ Certified Professional, Network+ Certified Professional and CCNA Module I. Having this educated and well-versed instructor cadre enables the school to instill in the students a collegiate training experience that utilizes IT industry standards.

BCOC is the 0602 MOS qualification training that prepares officers for the staff duties and responsibilities in entry-level billets. Twenty weeks in length, it focuses on mastering the fundamentals of communications techniques and skills pertaining to communications and data systems that are organic to the battalion- and squadron-level units in the MAGTF. Similarly, WCC is an eight-week MOS qualification training for the 0610 MOS (telephone systems officer), 0620 (tactical communication planning and engineer officer) and 0650 MOS (network operations and systems officer) to prepare them for staff duties and responsibilities as subject matter experts in their respective disciplines. ACOC is the MOS progression training for captains and majors to prepare them for staff duties and responsibilities in advanced-level communications billets on a G-6/general officer-level staff. During its 10 weeks, students are trained in the planning and technical employment of major subordinate command-level tactical communications systems and, upon completing the course, students receive the additional MOS of 0603 (advanced communications officer).

Regardless of the POI, each course includes extensive instruction in the following IT areas:

• Converging technologies and network services: exposes students to emerging technologies and services required by MAGTF commands. This study area focuses on services provided by single-channel radio networks such as chat and e-mail, beyond line-of-sight transmission systems, voice over Internet protocol, videoconferencing and virtual private network tunneling. It then delves into instruction on Internet protocol networking essentials, routing and switching technologies, and how to plan wide and local area networks. Further, students receive training on Microsoft Windows Server 2003 directory services, Microsoft Exchange, administration policies necessary for data management, disaster recovery, active directory replication, domain name system messaging services and Internet information services that satisfy the command's information and exchange requirements enabling command and control.

• Data network security: introduces students to the Marine Corps Network Operations and Security Center, the Marine Corps Enterprise Network and the network certification and accreditation process as well as the Information Assurance Manager Level One training levied by U.S. Defense Department Instruction 8570.1M. For the 0602 and 0650 students, the instruction includes the five-day CompTIA Security+ Professional training and certification exam.

Edson Hall is home to the Communications School.

Additionally, the courses provide a structured model for conducting communications planning through an introduction to the Marine Corps planning process. They also offer train-the-trainer concepts for developing a training plan for a communications unit. The culminating event for each course enables the students to apply their knowledge and demonstrate their ability to perform required skills while being closely evaluated by the instructing staff. The BCOC and WCC students each conduct a week-long field exercise during which they plan, install, operate and maintain complex and integrated tactical networks in support of scenario-based MAGTF operations. The ACOC students also engage in a scenario-based MAGTF operation and develop a communications plan for an operations order as well as conduct a confirmation brief for a notional Marine Expeditionary Force G-6 staff.

The officers graduate from their POI with an understanding of and appreciation for the realities of the 21st century C^4 operating environment. These communications leaders are prepared to embrace new information technologies and concepts and readily integrate them into the battlefield communications network in order to meet the commanders' demand for information at the right time and place.

Mission accomplished.

Lt. Col. Robert C. Wright, USMC, is the director, Communications School, Training and Education Command, Quantico, Virginia.

Marine Corps Warfighting Lab Enhances Capabilities Through Technology, Experimentation

By Brig. Gen. Robert F. Hedelund, USMC

The Marine Corps Warfighting Laboratory is a one-of-a-kind entity, combining innovation, experimentation and years of expertise to support current and future requirements of the Marine warrior. The Warfighting Lab performs concept-based experimentation to integrate operational concepts with tactics, techniques, procedures and technologies. These improve the expeditionary warfighting capabilities of the Marine Corps forces within the joint, coalition and interagency environments.

The lab's personnel includes recent combat veterans who have intimate knowledge of warfighter needs, scientists, technical experts and strategic thinkers. They make up the lab's seven distinct capability areas, and their vast experience is spread out across the lab, optimizing talents and skills sets. Since its inception in 1995, the laboratory, which is based in Quantico, Virginia, has conducted scores of diverse and challenging projects in support of the warfighter. These include the mobile trauma bay, immediate cargo unmanned aerial systems (UAS), enhanced company operations power and water, ground unmanned support system, experimental forward operating base, limited objective experiment 4, Banshee counter improvised explosive device systems, counter-sniper technology and fielded counter-bomber systems, and Expeditionary Warrior 2010, a scenario-based, multinational war game.

Two recurring themes resonate throughout Marine Corps Warfighting Lab efforts. First, the lab is working to "lighten the load" that Marines carry to improve their mobility, agility, survivability and endurance while reducing the occurrence of nonbattle injuries due to carrying heavy equipment loads. Second, "getting Marines off the road" aims at reducing Marines' exposure to improvised explosive devices and hostile ambush. The immediate cargo unmanned aerial system is another dimension of resupply tied to getting Marines off the road.

Immediate Cargo UAS

The Marine Corps is focused on assessing a near-term solution for an unmanned aerial vehicle (UAV) optimized for cargo delivery in the austere, forward-deployed environments of Southwest Asia. Referred to as the "Immediate Cargo UAS" project, this Marine Corp Warfighting Lab effort serves to demonstrate the state of the cargo (UAS) industry's current technological capability by evaluating the performance of several UAS. This approach will evaluate the overall abilities of those platforms to support near-term Marine tactical ground and aviation resupply requirements in an austere combat environment. The purpose of this effort is to establish a baseline for refining existing UAS technological capabilities, which can save the lives of Marines in combat as well as reduce the risk to ground forces by providing additional air options. The UAS can assume a portion of the combat resupply efforts currently performed by ground vehicles.

While cargo UAV concepts have been explored since the 1990s, the Marine Corps' recent transition from operation Iraqi Freedom to operation Enduring Freedom provided the impetus to further explore this need. Current efforts were developed as a direct result of guidance from the assistant commandant of the Marine Corps, Gen. James F. Amos, USMC: "Get trucks off the road."

Ultimately, this effort will help reduce the risk to our Marines and sailors engaged in ground logistics efforts by reducing the size and frequency of convoys along the unimproved and austere roads of Afghanistan. The near-term fielding of a viable cargo UAS also can supplement existing aviation resupply efforts conducted by manned assault support platforms, including rotary wing logistics and KC-130 aerial delivery sorties. This capability would increase the number of platforms and options available to a Marine Air Ground Force Task Force commander in overcoming the tactical logistics hurdle of combat resupply in an austere environment where there is a threat to ground vehicles. Such a capability also can provide a cargo delivery option in which resupply of forces is critical, but the environmental risk is high for manned air platforms.

Experimental Forward Operating Base

The threat of improvised explosive devices, the distance from secure logistics bases and the desire to reduce the risk of convoys being attacked in Afghanistan all contributed to a Headquarters Marine Corps decision to establish a recently chartered Expeditionary Energy Office (EEO). Another potentially life-saving initiative, the EEO charged the Marine Corps Warfighting Laboratory with simulating forward-

An immediate cargo unmanned aerial vehicle participates in the Marine Corps Warfighting Laboratory's Enhanced Company Operations, Limited Objective Experiment 3.3 at the Marine Corps Mountain Warfare Training Center in Bridgeport, California. The experiment's purpose was to help define unmanned or robotics technologies capable of remotely moving supplies— in whole or in part—to remote forward operating bases by ground transportation and to get Marines off the road.

deployed force energy and water demands and testing and evaluating alternative solutions to meet combat Marine needs in austere environments. The experimental base uses state-of-the-art science and technology to mimic the environments of operation Enduring Freedom's forward operating bases. The experimental team is charged with achieving three key objectives during a phased assessment. The first job is to assess and evaluate existing and proven commercial technologies to produce potable water onsite.

Another project goal is to increase the efficiency of power generation assets. The final goal aims at reducing the exposure of logistics-related convoys. By testing proven commercial technologies to produce potable water and improve fuel-consumption efficiencies, the Marine Corps will assess the baseline requirements of company-sized forward operating bases and determine how commercial off-the-shelf solutions can lighten the load of the combat Marines in Afghanistan. The Warfighting Lab supports current and future combat requirements for the Marine warfighter. Technology exploration is a key element of many lab projects.

For example, a recent limited-objective experiment focused on enhanced radio communications used to enable command and control (C^2) for enhanced company operations (ECO). These radios provided capabilities such as beyond line-of-sight, over-the-horizon, on-the-move, push-to-talk, netted Iridium and mobile ad-hoc networks (MANET). The Distributed Tactical Communications System (DTCS) is a surrogate technology that uses the low earth orbit satellite constellation. Battalions, companies and squads receive greater coverage by the low earth orbit constellation, allowing each to disperse and cover greater distances. Additionally, this technology provides the flexibility of going over or around obstacles as the satellites move overhead. These same obstacles traditionally will sever satellite communications. With a current range of approximately 100-150 miles and an extension package pushing the distance to 250 miles, this technology could ease the C^2 burden for complex operations. In future testing, this radio will be issued to squad and other senior leaders and will be installed aboard ships. Marines and soldiers in Afghanistan currently use the DTCS.

The Marine Corps Warfighting Lab uses TrellisWare, a software-defined radio, as a surrogate technology capable of creating a meshed, self-healing, self-forming, nodal MANET. Trellisware features digital-quality voice and provides eight simultaneous channels out to eight hops at a useable data rate of 220 kilobits per second. The ability to communicate and passively relay multiple channels greatly extends the battlefield and eliminates the need to relay to distant nodes. TrellisWare provides and displays grid location and automatic voice prompts when entering or exiting the network or changing channels. These capabilities are crucial to a Marine on the move.

Whether it is unmanned systems or more efficient processes for organizing the Corps' forces to meet diverse global missions, the Marine Corps Warfighting Laboratory tackles today's challenges to provide future solutions.

Brig. Gen. Robert F. Hedelund, USMC, is commanding general, Marine Corps Warfighting Lab.

What's In Your Service Catalog?

By Capt. Chris Granger, USMC, and Maj. Byron Harder, USMC

Information Technology Service Management and the Military

Since 1775, the U.S. Marine Corps has been making Marines and winning battles. We always have adapted our ability to train and fight as the technology of warfare matured around us. On today's battlefield, advantages are achieved through information superiority. Network-centric operations and warfare describe the goal of providing information to warfighters seamlessly so that end users do not require intimate knowledge of or involvement in the systems and networks used to deliver information.

The amount of information available is overwhelming; it only is useful when structured into services that are familiar to users. As information technology (IT) professionals, we must understand that these IT services are the fundamental purpose of networks and systems. Furthermore, unlike many physical weapons systems, military IT has tended to follow industry developments rather than pioneer them. To ensure that the delivery of services is accomplished in the most effective and efficient manner, we must adapt industry best practices to the military environment and manage the services we provide, not just the technology we procure.

The U.S. Defense Department (DOD) framework for accomplishing this mission is NetOps, or network operations, as outlined in DODI 8410.02. Compare this to what may be the most widely accepted framework for IT service management (ITSM) in industry today, the Information Technology Infrastructure Library (ITIL). Initiated by the British Office of Government Commerce, the ITIL emerged in the 1980s. Currently in version 3, the library is a best-practice framework that has been developed by both the public and private sectors internationally. It is a collection of recommendations for how IT resources should be organized and managed to deliver the best value to the customer through people, processes and technology.

The ITIL texts and the supplementary information provided by vendors provide a greater level of detail than the core NetOps documents do because these two concepts have differing purposes. NetOps is a directive framework for describing the operational authorities for the DOD's Global Information Grid. Since the DOD is a massive and varied organization, NetOps must remain sufficiently high level to be applicable across all its subordinate components. ITIL is a suggestive collection of best practices. By nature it is not mandatory for its readers, so its recommendations can offer more detail. In fact, it often describes mutually exclusive options. However, ITIL contains common themes and lessons learned that any organization needs to consider; the alternative is to head down a difficult path that others already have circumvented.

The scopes of NetOps and ITIL do not intersect completely. NetOps includes topics that ITIL does not, such as spectrum management and command and control, while ITIL considers supporting processes that NetOps does not, including financial and supplier management.

As a collection of recommendations, ITIL cannot be implemented or conformed to like an international standard. To gain some of the benefits of ITIL, an organization must establish an ITSM initiative. This activity is, essentially, a decision of what to establish and a tailoring of best practices to the organization's unique features. With 24 different processes, four functions, and a host of strategic and other recommendations, ITIL cannot be swallowed whole. Successful ITSM in any organization requires a significant culture change. It must have stakeholder buy-in at all levels. Implementing a single process to a desired level of maturity requires a great deal of management attention. There are costs associated with implementation: education, project management, procurement and upgrading of tools and systems, and external consulting. The changes may require new roles in the organization—which may increase or decrease the workforce. Changing the way that well-established technological experts perform their work is often a challenge. These changes take time and effort, which can be difficult to communicate to stakeholders. There is no shortcut to ITSM; despite vendor claims, there is no such thing as "ITIL in a box."

A key indicator of whether an organization is performing ITSM is the existence of a Service Catalog. That is, to manage its IT services effectively, IT must have a list of what the services are. Many organizations do not. Rather than organize around services, it is common to organize around technological components (systems, to use DOD parlance). This tends to obfuscate the issue of whether services are being delivered effectively, because services depend on the interaction of many components in different ways. A component that appears fully functional in isolation could still be a fault from an end-to-end perspective.

ITSM in the Marine Corps

The United States Marine Corps' ITSM initiative is called Enterprise Information Technology Service Management (E-ITSM). E-ITSM was created by joint decision of Headquarters, Marine Corps Com-

mand Control Communications and Computers (HQMC C4), Marine Corps Network Operations and Security Center (MCNOSC) and Marine Corps Systems Command (MCSC) to consolidate IT process development and tool acquisition efforts under a single project in response to the appearance of ITSM in multiple requirements documents. E-ITSM will be designated as a Strategic Sourcing Vehicle (SSV) for ITSM services and tools. Contractors performing work under E-ITSM will provide consulting, process development, tool configuration, training, and "early life support" for new capabilities but will not perform the actual management of IT. In the Marine Corps' Government Owned, Government Operated (GO/GO) model, the actual delivery of IT services is our internal responsibility. E-ITSM supports GO/GO efforts by providing a single resource point for processes, tools, and configurations across the Marine Corps Enterprise Network (MCEN).

E-ITSM has begun development of common ITSM processes. Using ITILv3 as a starting point and NetOps as a required framework, E-ITSM is tailoring best practice recommendations to fit the needs of the Marine Corps. The current focus of E-ITSM is the Secret Internet Protocol Routing Network (SIPRNET) and the Marine Corps Enterprise Information Technology Services (MCEITS) program (datacenter consolidation and application hosting), but the vision is to extend processes to the entire Marine Corps Enterprise Network (MCEN). E-ITSM will leverage lessons learned during early implementation through continual improvement and an increasing scope of development.

One of the first processes that the Marine Corps selected for development is the Service Catalog Management process. This development will produce the authoritative list of services, and eventually their required service levels, across the enterprise.

The three key Marine Corps authorities of Governance, Acquisition, and Operations (represented by HQMC C4, MCSC, and the MCNOSC) are generally mapped to the five ITILv3 lifecycle stages. The Governance community focuses on Service Strategy, the Acquisitions community focuses on Service Design and Service Transition, and the Operations community focuses on Service Operations. Continual Service Improvement is the responsibility of every organization.

IT Governance helps to ensure all stakeholders, including senior Marine Corps leadership, internal customers, and in particular divisions such as finance or legal, have the necessary input into the decision making process. IT Governance is the steering function that provides overarching policies and directions for IT in support of the Marine Corps' overall mission and assures adherence to legal and regulatory requirements.

IT Acquisition is responsible for designing, developing, procuring IT service material solutions, and providing subsequent Lifecycle Management support. IT Acquisition must adhere to legal and regulatory requirements and must develop systems that meet requirements specified by the Service Headquarters.

IT Operations is responsible for delivering IT services and enabling value to the customer in terms of supporting mission accomplishment. IT Operations is supported by IT Acquisition through provision of resources. This, in turn, is supported by the organization's strategic assets in the form of goals and objectives.

These descriptions highlight the fact that each community and all lifecycle stages are interdependent. For example, IT Acquisitions provides in-service support for services delivered by IT Operations and conducts procurement actions according to funds allocated by IT Governance. ITSM provides a mechanism to integrate organizations and statutory authorities performing Governance, Acquisition, and Operations within the Marine Corps. Cross-cutting, mutually agreed processes support delivery of IT services and capabilities. With iterative implementation of ITSM, NetOps authorities will be more and more focused on the warfighting and business needs of the customer and user bases. Common measurements of effectiveness will provide decision-makers the metrics they need to make effective resource decisions and meet objective service level requirements that correspond to the priorities of commanders. This will result in more efficient and effective IT services that are tightly integrated with the mission, helping to make information superiority a reality.

Capt. Chris Granger, USMC, is a network operations officer in the plans and policy division, Command, Control, Communication and Computers, Headquarters U.S. Marine Corps.

Maj. Byron Harder, USMC, is an Enterprise-Information Technology Service Management project officer, Marine Corps Systems Command.

---

continued from page 7

tic, preserve their ability to be responsive and rapidly insert new technologies for any number of reasons.

Industry Partnerships

To execute this evolutionary transformation effectively, we continue to work closely with our industry partners to identify and employ proven technologies. The Marine Corps will continue to leverage commercial technology, tools and industry practices to meet its unique mission requirements. The Marine Corps Systems Command employs innovative acquisition strategies to overcome the obsolescence created by today's rapid technology advancements, and it leverages industry expertise—especially in the areas of information technology and information management—to meet the needs of its customer—the warfighter.

Dr. John Burrow is the executive director for the Marine Corps Systems Command.

Find out more about the Marine Corps Systems Command by visiting: **www.marcorsyscom.usmc.mil/vendor/**.

Quantico-Potomac Chapter Supports Marine Corps Warfighters

AFCEA's Quantico-Potomac Chapter underwent a major revitalization in 2009 to support the active-duty and industry-based membership that supports the Marine Corps in Quantico, Virginia. The chapter has a history of strong active-duty membership, but there has been a change in the business strategy of major industry, including a broad relocation of business offices within Prince William and Stafford counties that are closely located to the Marine Corps customer at Quantico. As a result, there has been a shift in the membership base from predominantly active duty to industry membership.

By Mike Warlick

In order to meet the needs and requirements of the Marine Corps customer, the chapter president, Mike Warlick, reached out to Maj. Gen. George J. Allen, USMC, the director for Command, Control, Communications and Computers (C4), and the deputy Department of the Navy chief information officer for the U.S. Marine Corps; his deputy, James P. Craft; and the executive assistant, Col. Ron Zich, USMC, for guidance and to seek support for the chapter. Craft and Col. Zich, both strong AFCEA proponents, assisted the chapter by hosting a series of meetings to review how AFCEA can gain more relevance within the Marine Corps as a whole.

From these meetings emerged the chapter's theme for the 2009-2010 year: "the Role of the Marine Corps in a Changing Green and Security Information Technology (IT) Environment." This theme includes developing a strong working relationship with the Marine Corps Systems Command as a key component of industry support for Marine Corps requirements.

The chapter wasted little time in establishing an interim chapter executive committee, comprised of 12 industry and active-duty volunteers. The first order of business was to set chapter goals for events, establish a scholarship program, develop a membership campaign and begin a Young AFCEAN program. The chapter voted to undertake the following events: hold six annual events consisting of luncheons and industry-sponsored mixers; sponsor an annual scholarship golf fundraiser; and host an annual USMC IT Day. The first event was held in March and featured Gen. Allen as the guest speaker. This event set the tone for the chapter by demonstrating the C4 director's support.

By the end of 2009, the chapter's accomplishments included four luncheon events, two industry mixers, one scholarship golf tournament and the presentation of two $1,000 college scholarships to local high school students. The keynote accomplishment is the Quantico-Potomac Chapter-hosted USMC IT Day event, which takes place on April 27. This landmark event will highlight both IT operations as well as acquisition to meet the theme of the changing green and security IT environments within the Marine Corps.

Throughout 2009, the chapter was led by Warlick; Lt. Col. Jay Storms, USMC, chapter vice president; Steve Gaudreau, chapter secretary; and Andy Peters, chapter treasurer. Additionally, in less than three months, Mike Wallace established a scholarship committee and awarded two scholarships, and Don Brookins served as the chairman for the chapter's First Annual Scholarship Golf tournament, which was a success.

The Quantico-Potomac Chapter has198 active members and grew by 63 new members during 2009. Find out more about the chapter by visiting the Web site at www.afcea-qp.org. The 2010 schedule of activities is listed along with results of past events.

The officers of the revitalized Quantico-Potomac Chapter are sworn in. From l-r are Mike Warlick, chapter president; Steve Gaudreau, chapter secretary; William Wright and Lt. Col. Richard Leino, USMC, webmasters; and Andy Peters, chapter treasurer.

Mike Warlick is the president of the Quantico-Potomac Chapter.

For more information about AFCEA, visit the Web site at www.afcea.org. Visit the Quantico-Potomac Chapter's Web site at **www.afcea-qp.org**.

Marines trust Harris IT Services to unify their enterprise for cost-effective mission success

Harris IT Services designs, builds, and supports assured communications® solutions that enable government and commercial customers to meet their missions, on time and within budget. Leveraging Harris Corporation's long legacy of deep engineering expertise, IT Services is uniquely positioned to deliver end-to-end communications and IT solutions with speed and flexibility.

That's why our customers – including those in defense, intelligence, homeland security, civil, and commercial markets – rely on us to solve their difficult IT and communications challenges, as well as maintain those solutions 24/7/365.

HARRIS assuredcommunications®

Visit us online at www.itservices.harris.com

RF Communications • Government Communications Systems • Broadcast Communications • IT Services