

# On Cyber

## Preparing the 21st century MAGTF to fight in the cyberspace domain

by Capt Austin Duncan

The MAGTF is the Marine Corps' principal warfighting organization, a task-organized force tailored in size and capability to accomplish any mission across the range of military operations. The *Marine Corps Operating Concept*, published by HQMC in September 2016, asserts, "The 21st century MAGTF executes maneuver warfare through a combined arms approach ... across five domains—air, land, sea, space, and cyberspace." Currently, MAGTFs of all sizes and capabilities are unable to execute maneuver warfare through combined arms in cyberspace. To prepare for armed conflict in the cyberspace domain, the Marine Corps must stop conceptualizing conflict in cyberspace as a primarily defensive operation, enable MAGTFs with organic cyber capabilities, and demand an extension of cyber authorities to the tactical level in support of MAGTF operations. Should the organization evolve, the 21st century MAGTF can, and will, succeed in the cyberspace domain.

The essence of maneuver warfare is conducting both offense and defense, simultaneously and indiscernibly. To date, MAGTFs focus efforts in the cyberspace domain almost exclusively on defense of friendly communications networks and safeguarding information. What MAGTFs lack is an offensive capability or striking power. A critical component of any defense is the inclusion of offense, the threat of a decisive counterattack to seize the initiative. Similarly, an effective offense requires defensive characteristics to conceal the main effort and achieve surprise. Offense and defense must co-exist. Despite the recognition of cyberspace as a new domain, the principles of warfighting remain the same. Cyber professionals

**>Capt Duncan is the Technical Information Officer, Fires and Effects Coordination Cell, I MEF.**

are not only network defenders, but they must be armed and capable of transitioning from defense to offense, rapidly and unrelentingly. The Marine Corps cannot continue to emphasize network defense as the primary focus for MAGTF cyber professionals; it must make a concerted effort to also train and equip cyber warriors on offensive principles in order to gain and maintain the initiative in combat.

MAGTFs require *organic* cyber capabilities to conduct cyberspace operations in a contested-network environment. MAGTFs are currently unable to effectively operate in cyberspace because

of a limited number of cyber personnel, rudimentary equipment, and a lack of intelligence support. Present deficiencies are addressed through reachback agencies or an arduous request process for specialized support from the newly created Cyber Mission Force. These short-term fixes are not viable solutions for a forward deployed MAGTF operating in contested-network environments in the 21st century, especially against a potential near-peer adversary. Untimely support requests, technological restrictions on connectivity and bandwidth, and inherent security risks while communicating with a reachback entity represent only a fraction of total concerns. While the cyber mission force may serve as a viable force provider in the near term by attaching support teams, the Marine Corps' vision must be one which seeks a permanent cyber-force solution inherent within all sizes of MAGTFs.



**The principles of warfare haven't changed, but cyber warfare changes the operating environment. (Photo by LCpl Tojyea Matally.)**

To fight and win in the cyberspace domain, MAGTFs require organic cyber personnel and equipment.

The Marine Corps must lead the charge to extend limited cyber authorities down to the tactical level in

ranging from something as benign as network mapping or a denial-of-service attack at a local Wi-Fi to catastrophic permanent destruction of critical services. MAGTFs do not require broad cyber authorities, much like they do not

The Marine Corps must contest senior policy leaders' current stranglehold of cyber authorities. If left unchallenged, cyber authorities will remain at too high a level for a MAGTF to employ.

The 21st century MAGTF can win in the cyberspace domain. As the Marine Corps' premier organization, task organized to fight and win across the range of military operations, success in cyberspace is a no-fail mission for the MAGTF. To better prepare for future armed conflict, the Marine Corps must empower MAGTFs to assume the offensive in cyberspace, train and equip them with organic cyber capabilities, and aggressively seek delegation of limited cyber authorities to the tactical level. Evolving the MAGTF by preparing to fight in the cyberspace domain will ensure Marines continue to win in any clime and place.



---

***As the Marine Corps' premier organization, task organized to fight and win across the range of military operations, success in cyberspace is a no-fail mission for the MAGTF.***

---

support of the MAGTF. Critics allege that the inherently sensitive nature and complexity of cyberspace operations require authorities to reside at a very high level. This is a valid argument for *some* operations in cyberspace. However, cyberspace operations span a large continuum of complexity and destruction,

retain the authority to indiscriminately engage every target with all fire support assets. MAGTFs simply require limited authorities, captured within clear rules of engagement, to execute cyberspace operations on planned targets and targets of opportunity directly pertaining to the accomplishment of the mission.

— \$14.95/\$13.46\* —

**USMC GARDEN FLAG**

Flag Pole Sold Separately

[WWW.MARINESHOP.NET](http://WWW.MARINESHOP.NET)

\* member price only.

 **The MARINE Shop**  
Serving Marines Around the World  
Operated by the Marine Corps Association

  @themarineshoponline