

# A combined arms approach to defending Army networks

*By Russell Fenton*

In the face of new cyberspace challenges, we must adopt new ways of defending our networks.

If change cannot be enacted, we will find ourselves mired on the bitter trail of defeated militaries that failed to adapt to changing environments at the time and pace necessary.

We can hear faint rumblings and see the cracks in the walls of our network security. The defenses in confidentiality, integrity, and availability of the information modified, exchanged, and stored by Army networks and information systems is under continuous attack. The incident related to Operation Buckshot Yankee was only one “known” out of hundreds or thousands of “unknowns”; and in the end, terabytes (maybe even petabytes) of data are exfiltrated from Army networks on a yearly basis.

Now that we are fully aware of the continuous threats and some losses of security in cyberspace, we must use this opportunity to develop and gain support for a different approach to defending our networks against a myriad of threats.

Cyberspace is defined as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.” Given the inclusion of the terms “information technology infrastructures” and

“telecommunications networks” within the cyberspace definition, along with the fact that JP 6-0 (Joint Communication Systems) states “The GIG operates, through cyberspace, as a globally interconnected, end-to-end, interoperable network-of-networks...,” there should exist no doubt that Army networks are the land forces’ application of the cyberspace domain.

As it has for more than a decade, the Army depends on cyberspace [the LandWarNet] to function and create the necessary effects to gain an information advantage over adversaries of the U.S. It is difficult to overstate this reliance. Commanders and leaders at all echelons, whether CONUS or OCONUS, have come to rely on cyberspace to collaborate, gain situational awareness, plan, and conduct mission command at net speed through the full range of military operations. The Department of Defense has recognized this reliance on cyberspace; and subsequently in July 2011, it published a strategy that directs the services to treat cyberspace as an operational domain (as relevant a domain as land, sea, air, and space) to organize, train, and equip so they can take full advantage its potential.

No doubt our adversaries have recognized the Army’s ever-growing dependence on this new domain. Realizing they cannot match the Army force-on-force, nation states and terrorist groups alike are aggressively building capacity to fight us in the virtual realm. This fact foretells a future in which no other aspect of the Army will experience the reality

of persistent conflict more than the LandWarNet. It additionally leads to cyberspace becoming a distinct dimension for warfare in its own right. The warfighters and leaders of the U.S. Army will gain a significant advantage if it can defend the LandWarNet against internal and external threats. But to win that fight, Army leaders must implement a new operational approach that echoes proven land domain concepts in an abstract cyber battle space.

(Continued on page 20)



Cyberspace is a domain critical to mission command and daily operation. Defending cyberspace requires the same combined arms approach that has been successfully used in other aspects of military and domestic operations.

(Continued from page 19)

The success of American warfighters in the land domain has much to do with our ability to apply elements of combat power at the time and place of our choosing. The application of combat power requires a combined arms approach that integrates complementary, yet uniquely different, capabilities so that counteracting one makes the enemy vulnerable to another. ADP 3-0 provides an example of this approach when describing how commanders use artillery to suppress an enemy bunker complex, which then enables an infantry unit to close with and destroy the enemy.

Effectively defending the LandWarNet requires that Army warfighters expand our notion of where combined arms must be conducted. In the past, Army leaders viewed the LandWarNet as just an enabler to more efficiently meet information requirements. But combat power needs to be applied in cyberspace just as much as through it. Complementary, yet uniquely different, cyber capabilities across network build, operate, defend, exploit, and attack functions must be integrated in order to find, fix, and finish threats and vulnerabilities inside and outside the network. This does not mean that Army warfighters should do away with the primary objective of fighting and winning in the land domain (successfully defending in cyberspace must lead to a physical outcome). Instead, Army warfighters should recognize the fact that commanders have to leverage the appropriate capabilities as part of a combined arms approach in cyberspace similar to the more established paradigm.

Traditionally, commanders look to Signal elements for the installation, operation, maintenance, and defense of the organization's network. The availability of the network, along with the confidentiality and integrity of the information riding it, are assumed. Vulnerability alerts and network related tasking orders circumvent operations channels and are pushed down through more technical channels. Information about current threat tactics, techniques, and procedures which can be used to proactively implement appropriate countermeasures has been difficult to receive. The result of this has been reduced situational awareness, no unity of effort, and networks that have seen their fair share of exploits.

The idea of a combined arms approach to defend the network establishes a working environment which enables the coordination, integration, and synchronization between the operational processes performed in the current operations, future operations, and plans under an operations section – who disseminate and oversee the execution of the commander's priorities – with the unique network

operate and defensive capabilities provided by the Signal element, and the specialized intelligence, surveillance, and reconnaissance support and specific offensive cyberspace reach-back capabilities provided by the Intelligence community. All this enhanced by other information related capabilities such as inform and influence activities and even knowledge management. Similar to the combined arms example in ADP 3-0 that described the mutually supporting efforts of Field Artillery and Infantry, an example of combined arms in cyberspace would be the use of Signal-related capabilities to disrupt or redirect malicious activity away from critical net-enabled mission command systems, which then allows an Intelligence-related Cryptological Support Element to close with and destroy the enemy's cyberspace capabilities. Expanding network defense operations from the friendly to adversary box increases the situational awareness and unity of effort the Army lacks, and creates an economy of force that ensures commanders can concentrate network defenders when and where necessary.

For more than a year now, leaders in the Army Cyber Command Army Cyberspace Operations Integration Center at Fort Belvoir, Va. have been utilizing a combined arms approach to defend the LandWarNet at the strategic-level. Yet, a recent article by members of the U.S. Army Mission Command Center of Excellence at Fort Leavenworth, Kan. highlighted that to some degree, a combined arms approach is already taking shape at the operational and tactical-level as well. The soon-to-be-published revisions to Field Manual 3-36 Electronic Warfare in Operations will task the commander's EW element to expand and use the EW working group to facilitate the integration of what Army leaders call Cyber Electromagnetic Activities. The overarching objective of CEMA is to gain an advantage, protect the advantage, and place the adversary at a disadvantage in a congested and contested cyberspace and electromagnetic spectrum. However, the solution is intended only as a bridge until the Army develops a more appropriate means to achieve this. Army Cyber Command leaders and the MCCoE, supported by leaders from the Signal Center of Excellence and Intelligence Center of Excellence, amongst others, are working the Army's effort to determine how best to accomplish CEMA integration for the long term.

Current plans envision CEMA integrated within the operations process via the Cyber-Electromagnetic Working Group (consisting of the G/S-2, G/S-3, G/S-6, G/S-7, and others). The role of the working group will be to integrate and synchronize cyberspace operations, EW and EMSMO to maintain freedom of action in cyberspace while de-

nying our adversaries the same, ultimately to achieve the commander's operational objectives. This will involve unifying the offensive and defensive aspects of cyber-electromagnetic activities and orienting them on the commander's intent. To this end, the working group serves as the source of cyber-electromagnetic situational awareness and continually assesses progress toward desired conditions.

The first demonstration of the CEMA concept will occur during the Network Integration Evaluation (NIE) 13.1 (Oct-Nov 12) at Fort Bliss, Texas. Representatives from the SigCoE, Army Cyber Command, and MCCoE have already worked with the organizations supporting the evaluation (Brigade Modernization Command, 1st Armor Division, and 2/1BCT) to determine the appropriate network defense related functions that will be conducted in the work group by representatives from the S-6:

- Share and integrate the friendly network common operating picture with information on adversary and other specified cyberspace areas in order to produce overall cyberspace situational awareness
- Receive and request intelligence information from the S-2 in reference to potential threats and associated threat tactics, techniques, and procedures utilized against mission command networks and systems
- Assess, coordinate, and synchronize changes to the unit's information operation condition and

overall readiness level

- Plan, integrate, and synchronize network defense operations into the unit's operations processes and scheme of maneuver
- Report information on unauthorized network activity to be integrated with other possible indications and warnings
- Present a timely and accurate estimate of technical impact resulting from the threat activity and determine detrimental effects to the unit's mission assurance
- Plan, coordinate, and synchronize response actions to threat activity and assess risk for mission command networks and systems
- Plan, request, and coordinate the implementation of network defense capabilities provided by entities external to the unit
- Participate in the after actions review of an incident to determine the effectiveness and efficiency of incident handling
- Assist in the prioritization of CEM effects and targets
- Deconflict network defense operations with unified land operations, to include vulnerability assessments
- Support CEM TTP development
- Assess defensive CEM requirements
- Provide current assessment of network defense resources available to the unit

At least for the S-6, integrating these actions within the work-group alongside complementary functions from the S-3 and S-2 will elevate the commander's support, gain access to information that can proactively lead to the implementation of network defense

countermeasures, minimize risk by leveraging offensive cyber and intelligence capabilities to address threats for which no organic defensive solution exists, and achieve unity of effort. Undoubtedly, lessons learned captured during NIE will determine if the functions stated are correct in fulfilling these objectives.

In the face of new challenges, the Army is indeed losing the fight to defend the confidentiality, integrity, and availability of the information modified, exchanged, and stored by Army networks and information systems.

Recognizing the LandWarNet as part of the cyberspace domain opens the doors to new paradigms and methods to get at this problem. The Army's strength in the land domain undoubtedly comes from its ability to successfully integrate complementary capabilities as part of a combined arms approach. Defending cyberspace should be no different. The ACOIC and CEMA concept will go a long way in making combined arms in cyberspace a reality.

Only the future will indicate if Army leaders adapted at the right time and pace to avoid another painful lesson.

*Russell Fenton presently works as Department of the Army Civilian as the Chief of the Cyber Cell, TRADOC Capabilities Management Office Global Network Enterprise, U.S. Army Signal Center of Excellence at Fort Gordon, Ga. He is a retired Signal and Information Systems Management (FA53) officer with over 24 years of combined service.*

## ACRONYM QuickScan

**ACOIC** – Army Cyberspace Operations Integration Center  
**CEMA** – Cyber Electromagnetic Activities  
**CONUS** – Continental United States  
**DoD** – Department of Defense  
**EMSMO** – Electromagnetic Spectrum Management Operations

**EW** – Electronic Warfare  
**GIG** – Global Information Grid  
**MCCoE** – Mission Command Center of Excellence  
**NIE** – Network Integration Evaluation  
**OCONUS** – Outside Continental United States  
**TTP** – Tactics, Techniques, and Procedures