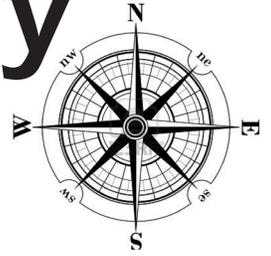


The Future of Military Mobile Computing



By COL Bruce Caulkins

Significant and enduring are two words that reflect the reality we face today regarding mobile computing technologies.

The ubiquity of smart phones, tablets, and other mobile computing devices in the commercial world makes cellular technologies a must for the future military network to support. The wide use of Smartphones also ensures that any potential users – especially those military users who are under the age of 30 – are more comfortable with the technology and therefore easier to train and understand how to use this new technology on the battlefield.

Currently, these technologies' vulnerabilities prevent us from

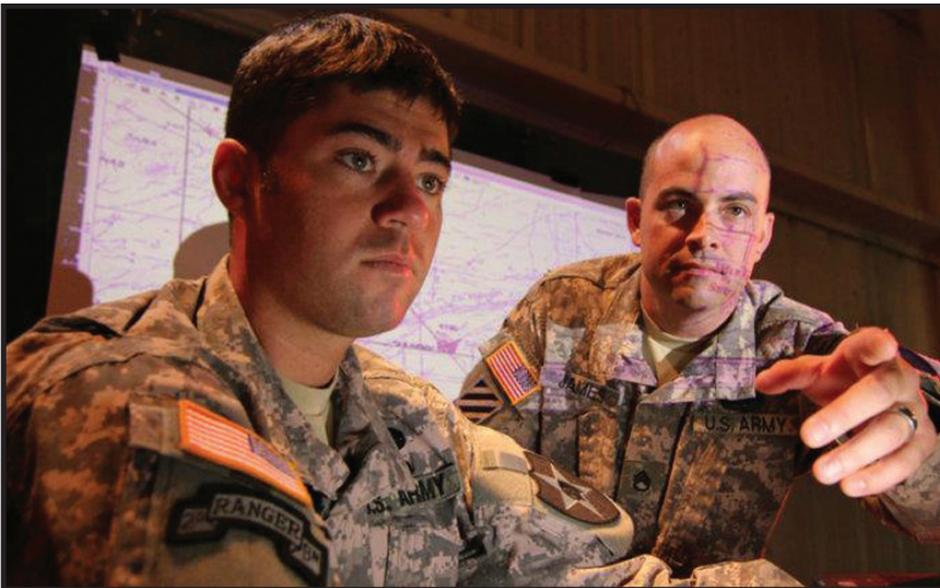
using most of these devices for official work. Cyber vulnerabilities exist that do not yet allow the military to fully use smart phone technology on the military network, or Global Information Grid. Common Access Cards, Federal Information Processing Standard 140-2 certifications, and software compliance are just a few of the hurdles that we need to overcome to make cellular technology a reality.

Cultural bias is also an issue. Everywhere in the federal government, you can talk to the leaders and engineers in any agency and they will tell you that they are excited about this technology and that they will support any action to get smart phones and apps onto our networks. Then, you can walk

down the hall in that same agency and the security folks will tell you that they can't see smart phone deployment happening any time soon, if at all. While the security professionals certainly have a legitimate point, "just saying no" is not a viable course of action any longer. Too many leaders and Soldiers are demanding this capability in garrison and on the battlefield. So we need to continue moving forward.

Last year, the Signal Center of Excellence published a cellular vision paper for the Army that outlines future steps the Army must make to move forward in this area. The paper can be downloaded at http://www.ecrow.org/pdf/Army_Cellular_Capability_Development_Strategy_16_August_2011.pdf. In that document, we proposed an integrated strategy that will give the Army the following capabilities:

- Ensure an effective, cost saving expenditure of resources, while eliminating redundancies and developing a solution that meets Warfighter needs
- Develop dynamic, secure smart phone software applications to provide ease of use and enhancements to Soldier use of handhelds or tablets
- Connect the mobile and dismounted Soldier to the network through an integrated solution
- Develop cellular technologies that can deliver high throughput at a low cost in a scalable, easy to deploy, easy to operate network architecture
- Exploit emerging cellular/broadband technologies and leverage commercial communications infrastructure for units both in garrison



(U.S. Army photo)

Soldiers utilize Distributed Common Ground System-Army, or DCGS-A, operations center at Aberdeen Proving Ground, Md. U.S. Army Research, Development and Engineering Command's communications-electronics center's Intelligence and Information Warfare Directorate hosts the Tactical Cloud Integration Lab in an effort to expedite cloud computing technologies to the Soldier.



(Photo by SSG Joshua Ford)

LTC Mark Stiner (*left*), program manager for the Joint Tactical Radio System Handheld, Manpack and Small Form Fit, shows GEN Peter W. Chiarelli, the Army vice chief of staff, how to operate part of the JTRS during a training event with Paratroopers from Company C, 1st Battalion, 505th Parachute Infantry Regiment, 3rd Brigade Combat Team, 82nd Airborne Division, at Fort Bragg 3 March.

and while operationally deployed

- Initiate phased insertion of commercial wireless technologies, interoperable with tactical networks, and complementary to programs of record, with legs to future (WIN-T, JBC-P, Nett Warrior, and JTRS)

- Implement an Army unified communications strategy, designed to enhance garrison/mobile networks through efficiencies in delivery and routing of voice, video, data through network convergence.

These seven imperatives plot the way for the future. While recognizing the cyber vulnerability

issues, they also show that inserting various commercial wireless and cellular technologies into specific programs of record will allow mobile computing technologies to flourish and support those various programs of record's missions.

To accelerate these and other advanced communication capabilities into the force, the Army has created the Network Integration Evaluation at Fort Bliss, Texas. The NIE exercises are conducted twice per year and are designed to integrate and dramatically advance the Army's tactical network. To do so, the Army's Brigade Modern-

ization Command, in conjunction with the Army Test and Evaluation Command and Systems of Systems Integration Directorate, accomplishes the NIE exercises in order to conduct integrated and parallel Operational Tests of select Army programs of record. Further, the BMC and its partners use the NIE to evaluate development and emerging network capabilities in an operational environment and to assess non-networked capabilities in an integrated operational environment.

From the outset, the NIE has been a vital player in assessing mobile computing capabilities, both within programs of record-type systems and within stand-alone systems under evaluation. These future mobile computing capabilities will allow the Army to better support the needs of the commander all the way down to the individual Soldier, whether in garrison or in an operational environment.

COL Bruce Caulkins, Ph.D. is the G6 for the Signal Center of Excellence at Fort Gordon, Ga. He is a Signal Corps Functional Area 53 Information Systems Management officer and has recently served as the chief of the Accelerated Capabilities Division, the commandant for the Leader College for Information Technology, and the director of the School of Information Technology. He has written numerous articles in the cyber and cellular areas and his doctorate is in Modeling and Simulation, focusing on network security.

ACRONYM QuickScan

ATEC – Army Test and Evaluation Command
 BMC – Brigade Modernization Command
 CAC – Common Access Card
 FIPS – Federal Information

Processing Standard
 GIG – Global Information Grid
 JBC-P – Joint Battle Command – Platform
 JTRS – Joint Tactical Radio System

NIE – Network Integration Evaluation
 SIGCoE – Signal Center of Excellence
 SoSI – Systems of Systems Integration