Modernizing the Force

Implementing Policies...

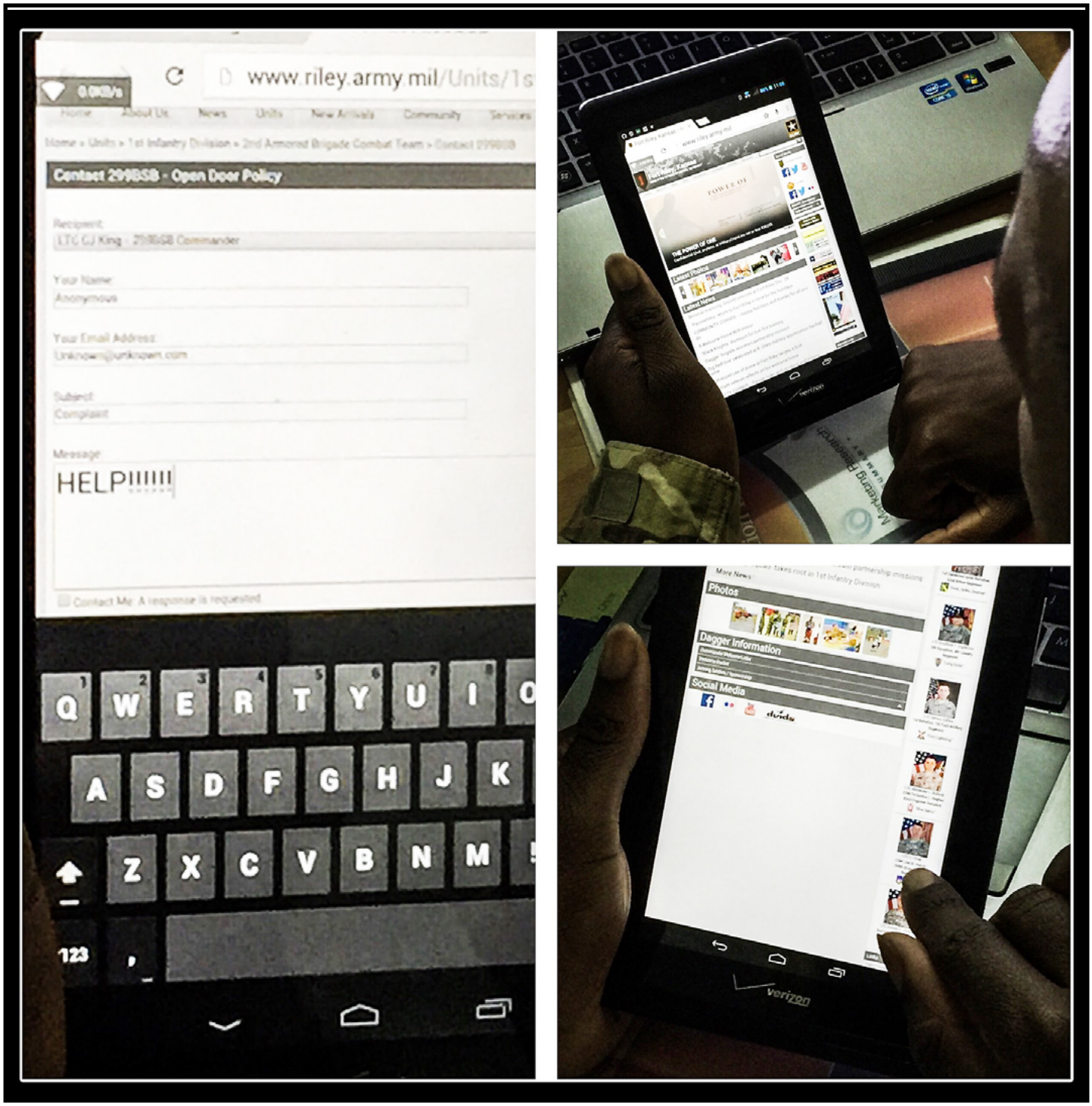
By CPT Trenin D. Spencer,
SFC Christopher L. Donald
SPC Ashley M. Ardiana

Computers have the ability to maximize work efficiency while reducing the costs of operations, which makes emerging military computer applications and ideas to leverage existing technologies for multiple military uses extremely desirable for our military.

From battle tracking, fires integration, and airspace de-confliction to personnel management, education, and training management, the U.S. military has already integrated computers into the majority of its daily operations and will move to do so on an even greater scale as the ever evolving threat to our country mushrooms across all technology-enabled pathways.

(Continued on page 10)

...Electronically



(Above top right) **A Soldier uses a personal electronic device to access the Open Door Policy via the Fort Riley, Kansas official webpage.** ***(Above left)*** **The picture displayed on the personal electronic device is of a filled in contact form.** ***(Bottom right)*** **The picture displayed on the personal electronic device is of the battalion commander's page located on the Fort Riley, Kansas official site.**

(Continued from page 8)

As our military continues to modernize through the integration of computer technologies into daily operations, the implementation of military policies using electronic means is the future of the Army, and the exercise of the universal policy letter #1: Commander's Open Door Policy, utilizing the existing army enterprise email infrastructure, is the first leap toward that future.

Recently LTC C.J. King, battalion commander 299TH Brigade Support Battalion, 2ND Armored Bridge Combat Team, 1ST Infantry Division, made the comment that he felt "his open door policy was not effective, because it was not being utilized" and wished there was a better way to implement the policy.

Across the military, there is a shared misconception that as long as the door to the commander's office is open and the commander is not otherwise engaged, then the commander's open door policy is being exercised, and if Soldiers have legitimate issues, they will recognize the open door and address the issues.

As it turns out, that is definitely not the case as there are several barriers that deter Soldiers from exercising the open door policy. Those barriers most notably include intimidation of raising concerns to O-3 and above Officers and E-8 and above Noncommissioned Officers, and also fear of reprisal from the Soldier's immediate supervisor. As a result of LTC King's comment, SFC Christopher L. Donald (communications chief for the 299TH Brigade Support Battalion, 2ND Armored Bridge Combat Team, 1ST Infantry Division) devised a method for Soldiers to use the battalion commander's open door policy anonymously by accessing the publicly available official Fort Riley, Kansas, 1ST Infantry Division, "BIG RED ONE" website, and clinking on a hyperlink located on the battalion commander's command profile, which sends an unaddressed email to his army enterprise email address. This method of exercising the open door policy is not only completely confidential between the Soldier reporting and the battalion commander, but unless the Soldier chooses to include contact information in the message of the email, there is also no way for anyone else to know who exercised the policy. Due to the immediate success of the electronic form of open door policy, the battalion command sergeant major, company and battalion commanders across the division, and a commander in the Air Force all requested similar programs within weeks of our implementation.

Following implementation, it was quickly found that the ability to send anonymous emails to the battalion commander not only eliminates the intimidation and fear of reprisal barriers that Soldiers face, but it also provides the battalion commander with insight that he might not gain through vocal conversation due to a Soldier's inability to express him or herself orally. Other benefits discovered as a result of the electronic implementation of the open door policy include the increase in availability of the commander to address issues and the ease of use to exercise the policy for all Soldiers.

Commanders are busy Soldiers! Prior to the electronic implementation of the open door policy, the battalion commander was only available to discuss issues for potentially an hour during the duty day, and maybe an hour or two afterwards. The electronic open door policy completely removed time restrictions to address issues. All commanders have government issued personal electronic devices, such as Blackberry or iPhone devices, literally attached to their hips almost twenty-four hours a day. The electronic devices, coupled with the electronic open door policy, gives commanders immediate and twenty-four hours access to Soldiers who choose to utilize the open door policy.

Prior to the electronic implementation of the policy, geographical location limited the use of the open door policy. Soldiers who operate away from the flagpole, and who do not have the opportunity to interact with the command on a daily basis do not posses the ability to exercise the traditional open door policy and bring up the issues that often arise in isolated environments.

The electronic open door policy diminishes the effect of geographical separation and increases the ease of use of the policy for all Soldiers, because it only requires internet connectivity, a commonality for Soldiers to possess twenty-four hours a day in this age of the computer.

The electronic open door policy is easily integrated into standing policies. To set up your electronic open door policy you simply need to follow these steps:

1. Coordinate the creation of an email distribution list containing your policy owner/ owners information (battalion commander, command sergeant major, etc.) with your installation's Network Enterprise Center by submitting a work order. Your NEC will coordinate with the Army Enterprise Service Desk and reply with the work order that is created in order to begin the process. It takes about 3-5 business days for the distribution list to be created. As a best practice, your local automations personnel (S6) should manage the distribution list once it has been created.

2. Once you receive the email stating that the distribution list has been created, you need to contact your installation public affairs office web administrator. The PAO web administrator is in charge of managing your installation's official web page. From your PAO web administrator, you will request the creation of a hyperlink that accesses a web based contact card or form using the policy owner's name. The contact card/ form will contain the following information:

i. RECIPIENT: choose the policy owner, or if multiple leaders are using the same link, you may choose your leader of choice via dropdown menu;

ii. YOUR NAME: you may put anonymous or your own name if you would like to make the recipient aware of whom he or she may contact;

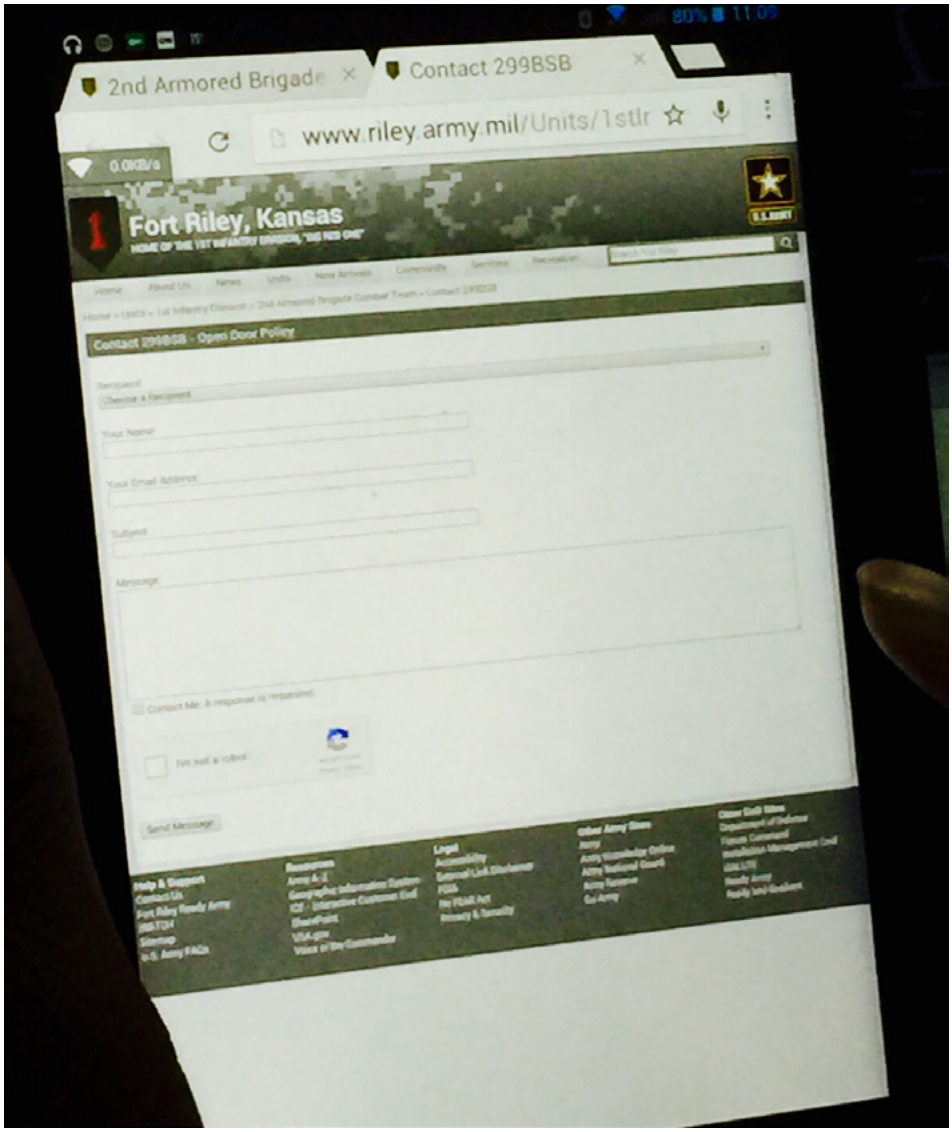
iii. YOUR EMAIL ADDRESS: you may either use your government email address, a personal email address, or a completely fake email address;

iv. SUBJECT: The concern you would like to make known to the recipient;

v. MESSAGE: Explanation of the concern and what suggestions you have regarding the concern.

3. The hyperlink is to be located on the policy owner's unit's official page. As a best practice, locating the hyperlink beneath the official command photograph allows for quick and simple access, without the hassle of searching every inch of the webpage. The link takes approximately 3-5 business days to be fully operational.

4. Finally, after you have received an email stating the link is good to go, you will then need to test the link. As a best practice, initially you must hold the control button and refresh the web page at the same time to get the link to work properly. Once the link for the contact card/form is up and running, you will then be able to post how-to instructions throughout the unit to show Soldiers how



This display shows how a Soldier can use a personal electronic device to access the Open Door Policy via the Fort Riley, Kansas official webpage. The picture displayed on the personal electronic device is of a blank contact form.

(Continued on page 12)

(Continued from page 11)

to utilize the new open door method.

Best practices to ensure widest dissemination of the electronic open door policy include flyers posted in all work and barracks areas detailing instructions on how to access the anonymous email hyperlink, briefings on the policy at weekly closeout formations, and even the Family Readiness Group channels.

In addition to reminding Soldiers about the policy during the weekly closeout formation, using that time to acknowledge receipt of issues brought up as a result of the open door policy, and to request additional information in order to action issues of major concern are also proven best practices.

Overall, the electronic open door policy is easy to manage and enjoys seamless integration with current policies, however it does require some overhead maintenance. It is important to ensure that email configurations are reconfigured with changes in command or key personnel, or else you end up standing tall in front of a very upset command sergeant major attempting to explain why the prior command is being notified about issues within the current command.

There is no mistaking that this is the age of the computer. Computer technology, which is nowhere near the pinnacle of its potential, will continue to shape the battlefield for decades to come. Soldiers of the 1ST Infantry Division, Big Red One or BRO Soldiers, understand and embrace this at every level. 1ST Infantry Division Commanding General, MG Wayne W. Grigsby, uses a commander's digital dashboard to post information and enable dialogue while flattening the organization, BRO leadership use computer technology such as the Digital Training Management System and the Army e-Learning Program to manage and supplement training, and BRO Soldiers use computer technology such as the Engagement Skills Trainer and convoy simulators to maintain lethality and readiness, making the 1ST Infantry Division the most Brave, Responsible, and On Point division in the Army. The exercise of Army policies via electronic means is here, and the electronic open door policy is the first of many polices to come as our Army continues to advance in this age of the computer.

Acronym QuickScan

ABCT – Armored Brigade Combat Team
BRO – Big Red One
FA – Field Artillery
LAN – Local Area Network
LTC – Lieutenant Colonel
NEC – Network Enterprise Center
NCOIC – Non-Commissioned Officer In Charge
PAO – Public Affairs Officer

2nd Armored Brigade Combat Team
"Dagger Brigade"

CPT Trenin Spencer *is the communications officer for the 299th Brigade Support Battalion, 2nd Armored Brigade Combat Team, 1st Infantry Division., Fort Riley, Kansas. He previously served as the signal company commander for the 2nd Armored Brigade Combat Team, and the communication's officer for 1-7 FA, 2ABCT, 1ID. His deployments include Kuwait, Malawi, Mauritania, and Iraq.*

SFC Christopher Donald *is the communications section chief for the 299th Brigade Support Battalion, 2nd Armored Brigade Combat Team, 1st Infantry Division, Fort Riley, Kansas. He previously served as the platoon sergeant for G6, 21st Theater Sustainment Command, Kaiserslautern, Germany. His deployments include 2x Kuwait, 3x Iraq, Bosnia, and Kosovo.*

SPC Ashley Ardiana *is the senior local area network manager for the 299th Brigade Support Battalion, 2nd Armored Brigade Combat Team, 1st Infantry Division., Fort Riley, Kansas. She previously served as LAN manager for Headquarters and Headquarters Battalion, 2nd Infantry Division, Camp Red Cloud, South Korea.*