



# Insight

Volume 4, No. 6

U.S. Army Intelligence & Security Command

April 30, 2004

## INSCOM working smarter

Our Army and joint forces continue to perform magnificently in the face of the Global War on Terrorism.

We're meeting the combined challenges of smart, adaptive, non-traditional adversaries; their ability to leverage first-world technologies; and the world's easy access to multiple terabytes of information about our country - a natural side-effect of our history of democratic and media freedom. We're getting this tough work done with a third fewer Soldiers than we had on our books during Desert Storm in 1991.

Today, INSCOM has over 750 Soldiers and DA Civilians deployed in 30 nations, in addition to thousands forward stationed. This is INSCOM's share of our Army's commitment of over 320,000 Soldiers deployed in over 120 countries worldwide.

Success continues to grow from enhanced situational awareness and our ability to generate actionable intelligence as mandated by the Chief of Staff's Focus Area 16. The importance of INSCOM and intelligence has never been greater.

In the coming months, we need to increase the volume of

actionable intelligence INSCOM delivers - and we won't get this done by simply working harder. We're already operating 24 x 7 at many places across INSCOM. We also need to work smarter by evolving the industrial age processes we inherited into a truly informational age configuration. It's not an option, we won't win the war on terrorism without leveraging horizontally integrated intelligence from both forward collectors and across the greater intelligence community. INSCOM, as the Army's operational intelligence force and joint team member, has a major role to play. Recently, key INSCOM leaders met to assess where the command is in this regard, and to chart a "way-ahead" for the next 18 months. Finalized priorities and milestones are expected in May, but a number of points are worth early review. I want to ensure that every member of INSCOM is on-board as we move forward.

Our Army is transforming its culture, mindset and structure towards a more rapidly deployable, modular force with enhanced processes. This will involve resetting every maneuver division, brigade and battalion over the next four years with significantly more intelligence



*DA photo*

capabilities. It will also mean digitally connecting them to national intelligence frameworks. This reset will permit INSCOM theater intelligence brigades and groups (TIBs and TIGs) to leverage horizontally integrated databases in support of tactical overwatch, another priority, for designated tactical divisions and maneuver brigade and battalion forces. INSCOM TIBs and TIGs will perform overwatch as a discrete, downward-focused mission task in support of Army Component and Army Service Component Command (ASCC) commanders. Bridging software will let us representationally merge and visualize previously restricted intelligence into

*(continued on page 2)*

(continued from page 2)

tactically useful domains. Built around a network of analytic centers, tactical overwatch will provide enhanced situational awareness - tailored, fused assessments, with target cueing and warning - at useable classification levels.

Army reset actions over the next four years will also increase the number of military intelligence Soldiers at maneuver brigade and battalion levels, and pose significant training challenges. INSCOM will be heavily involved in addressing these challenges under a proposal called *Foundry*. Under this concept, a percentage of intelligence Soldiers assigned to combat units of employment at the higher tactical headquarters and capabilities based unit's of action maneuver units would be stationed for three-year periods, with their families, at regionally dispersed INSCOM TIBs and TIGs. These INSCOM major subordinate commands will integrate *Foundry* Soldiers into ongoing live environment signals intelligence, human and counterintelligence, and analysis missions worldwide; broaden their experience and wartime skills; and return more capable military intelligence teams to their parent maneuver "owners" for scheduled major training events and contingency deployments.

Today's less structured threat environment also makes it necessary for us to change the methods with which we assess enemy behavior. We

must learn to routinely red team (RT) ourselves; see ourselves through the eyes of our enemy, in order to holistically assess proposed blue force status and operations, identify weaknesses, war-game mitigating solutions, and determine second and third-order effects. INSCOM will be the Army's operational lead for RT efforts and stand up a core group in the fourth quarter of fiscal year 2004.

That group will be comprised of full-time threat and functional experts - information operations, special operations, logistics and others - who will leverage a broader network of regional, cultural and other subject matter experts from across the Army and intelligence community. We will organize a similar, smaller RT capability within each TIB and TIG to support ASCC and task force planning. INSCOM will concurrently establish close links to TRADOC and the schoolhouse in order to capture RT lessons learned and incorporate that data into red team training modules now being designed as part of a formal instruction process.

Existing intelligence horizontal integration capabilities will advance in 2005 through the second phase of INSCOM's Pacific-based *Morning Calm* experiments. This nationally chartered effort applies cutting-edge software solutions and processing techniques against live intelligence problems of direct relevance to forces in the Pacific. *Morning Calm II* will provide the basis for lateral

transfer of proven techniques for use against GWOT and other significant intelligence problem sets.

As we continue with ongoing efforts to fully operationalize our headquarters, reinvest in our most critical warfighting support functions, and realign around enduring operational priorities, we will ensure that we still take care of our most precious resource - our people. We are powerfully assisted in these tough tasks by our strong linkage to our National Guard and Army Reserve components. The recent establishment of the Army's Military Intelligence Reserve Command within our headquarters will significantly help in this process.

It's an exciting time to be an intelligence Soldier or DA Civilian. Out Front!

**Maj. Gen. John F. Kimmons**

INSCOM Insight is published bi-weekly as a Command Information e-publication for the men and women of the U.S. Army Intelligence and Security Command under the provisions of AR 360-1.

Opinions expressed herein do not necessarily reflect the views of Headquarters, INSCOM, the U.S. Army, or the Department of Defense. All photos are U.S. Army photos unless otherwise noted.

Send articles, photographs, graphics or story ideas to INSCOM Public Affairs Office at [pao@inscom.army.mil](mailto:pao@inscom.army.mil), or copies to 8825 Beulah St., Fort Belvoir, VA 22060. For additional information, call (703) 428-4965.

**Maj. Gen. John F. Kimmons**  
Commanding General, INSCOM  
**Deborah Y. Parker**  
Chief, Public Affairs  
**Sgt. 1st Class Terry J. Goodman**  
Senior Public Affairs NCO  
**Brian Murphy**  
Editor

# Looking for a few good runners

by **Karen Kovach**  
INSCOM History Office

The Susan G. Komen Breast Cancer Foundation was founded on a promise made between two sisters - Susan Goodman Komen and Nancy Goodman Brinker.

Suzy was diagnosed with breast cancer in 1978, a time when little was known about the disease and it was rarely discussed in public. Before she died at the age of 36, Suzy asked her sister to do everything possible to bring an end to breast cancer.

Nancy kept her promise by establishing the Susan G. Komen Breast Cancer Foundation in 1982. Today, the Komen Foundation is a global leader in the fight against breast cancer; its mission is to eradicate breast cancer as a life-threatening disease by advancing research, education, screening and treatment.

The *2004 Komen National Race for the Cure*, a 5K event, will return to the streets of Washington, D.C., June 5, and for the fifth year, the INSCOM Federal Women's Program committee invites INSCOMers to participate as a team. Registration forms are available from the INSCOM EEO Office team captains Anne Bilgihan (703-428-4479) and Karen Kovach (703-706-1638). Registration is \$25.

Since 1990 the *Komen National Race for the Cure* has grown exponentially—from 7,000 participants to over

70,000. A minimum of \$1 million from the proceeds of the race remains in the National Capital Area to provide funding for breast health and breast cancer education, screening, and treatment programs; remaining proceeds directly support breast cancer research

through the Komen Foundation's Award and Research Grant Program.

Even if you can't participate in the race June 5, please consider registering to donate to the Komen Foundation and to support INSCOM's goal of at least 30 registrants.



photo by Bob Bills

**The U.S. Army Intelligence and Security Command Memorial Day ceremony is scheduled for May 20 at 10 a.m. in front of the Nolan Bldg., Fort Belvoir, Va. During the ceremony, INSCOM will honor 10 deceased Soldiers by adding their names to the INSCOM memorial statue in front of the Nolan Bldg.**

# Be careful what you download

FORT HUACHUCA, Ariz. (Army News Service) People spend hours in front of their computer screen, downloading music or new movies from the Internet, and not paying a cent. The Army considers such action on government computers to be a security threat.

One program that is used to download files is Peer-to-Peer (P2P) architecture. It is a type of network in which each workstation has the capability to function as both a client and a server. It allows any computer running specific applications to share files and access devices with any other computer running on the same network without the need for a separate server. Most P2P applications allow the user to configure the sharing of specific directories, drives or devices.

"The idea of someone else getting unfettered access to anything of yours without your explicit consent should scare anybody and that's exactly what P2P authorizes," says Zina Justiniano, an intelligence analyst with the U.S. Army Network Enterprise Technology Command's (NETCOM) Intelligence Division, G2. "P2P is freeware. Freeware, shareware most of the stuff that you pay nothing for, has a high price. The fact that it's free says that anybody and their cousin can get it; that means that anybody and their cousin can get to your machine."

P2P applications are configured to use specific ports



photo by Pvt. Daniel D. Meacham

**Downloading Peer-to-Peer software on a government computer is illegal.**

to communicate within the file sharing "network," sometimes sidestepping firewalls. This circumvention creates a compromise and potential vulnerabilities in the network that, in a worse case scenario, can lead to network intrusions, data compromise, or the introduction of illegal material and pornography.

There is also the issue of bandwidth. Since the start of the global war on terrorism, the most pressing issue from service members in the field is a shortage of bandwidth to transmit battlefield intelligence to combatant commanders. The average four-minute song converted into an audio file recorded at 128-bit, can be upwards of 5 megabytes. Full-length video MPEG files can easily reach 1.6 gigabytes. Depending on the connection speed, even a small file may take several minutes to hours

to download, using valuable bandwidth.

Unauthorized use of P2P applications account for significant bandwidth consumption. It limits the bandwidth required for official business, and storage capacity on government systems.

While those who monitor the Army networks agree that copyright infringement is a valid issue, they do have other, more important concerns.

There are several known Trojan horses, worms and viruses that use commercial P2P networks to spread and create more opportunities for hackers to attack systems. Trojan horse applications record information and transmit it to an outside source. They can also install "backdoors" on operating systems, transmit credit card numbers and password - making these

*(continued on page 5)*

*(continued from page 4)*

malicious programs a favorite of hackers. Some of the malicious codes allow hackers to snoop for passwords, disable antivirus and firewall software, and link the infected system to P2P networks to send large amounts of information (spam) using vulnerabilities in the Windows operating systems.

"If it's a really good Trojan horse, it will actually run two programs; it will run the program they said they were going to run, so they will not only download it, but they will install it and be very happy that it's there," Justiniano said. "Meanwhile in the background, another program is doing mali-

cious damage to the computer by either damaging files or possibly taking files off the computer without your knowledge. If it's a really nice program that runs well, (the user) will pass that file over to someone else because they really got their money's worth out of it. People will just keep passing it along."

The Army's regulation on Information Assurance, Army Regulation 25-2, specifically prohibits certain activities; sharing files by means of P2P applications being one of them.

There are some individuals who continue to use P2P applications on their Army systems.

Over a two-month period at the end of last year, government organizations identified more than 420 suspected P2P sessions on Army systems in more than 30 locations.

It seems some don't understand or haven't read the standard Department of Defense warning that says, "Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring."

For those who think, "How are they going to know it's me? I'm just one person in a network of hundreds of thousands," don't be surprised when network access is cut off and the brigade commander is calling.



*photo by Spc. Felicia Thompson*

**Sgt. Angela Falu, an HHC, 513<sup>th</sup> Military Intelligence Brigade mail clerk, is given a certificate with the NCO Creed at the 513<sup>th</sup> MI Bde Noncommissioned Officer Inductee Ceremony, April 2, at the Signal Theater. It is an Army tradition for the Soldiers' command sergeant major to first sign the document and then present it to the Soldier to sign.**

# Message for INSCOM civilians

Following the 9/11 tragedy, civilian employees have increasingly been called upon to deploy side-by-side with their military compatriots in support of military contingencies such as Operations Iraqi Freedom and Enduring Freedom.

Due to unforeseen circumstances, it may be necessary to identify civilian positions for deployment that have not previously been identified as such.

INSCOM is committed to minimizing the number of involuntary civilian deployments, and will ensure all personnel who are sent to perform combat support or other crisis-essential functions are provided with proper training, equipment, and protection.

To that end, INSCOM has developed a Civilian Deployment Guide which will be accessible on the INSCOM homepage in the near future.



photo by Sgt. Kyran V. Adams

***Like Soldiers, INSCOM civilians can find themselves on the ground in Iraq.***

For additional information regarding civilian deployments, contact Karen Wolfe at 703-428-4628.

## INSCOM Soldier earns Miller award

Chief Warrant Officer 3 Steven Pilkington, an instructor at the Department of Defense Polygraph Institute (DoDPI), earned the 2003 David Miller Most Valuable Player Award March 4.

Pilkington is an instructor detailed to DoDPI from the U.S. Army Intelligence and Security Command.

Pilkington was recognized for his contributions in the research, development, and testing of a passive device

designed to preclude the use of countermeasures in an attempt to defeat the conduct of a polygraph examination. This device is now in wide use throughout the Departments of Defense, Justice, Homeland Security and in other counterintelligence agencies. His efforts garnered a significant cost savings for these devices as compared to what private manufacturers charge the Federal government for similar devices.

The Miller award, named after a former member of the DoDPI Instruction Division, is awarded to a person, nominated by non-supervisory personnel and chosen by a committee. In the spirit of the steadfast manner in which Miller performed his duties and exhibited concern for his fellow workers, the award is given to the person who best exemplifies the traits exhibited by Miller, according to information released by the institute.

### Open season

The open season for the Thrift Savings Plan (TSP) began April 15, and will continue through June 30. Federal Employees Retirement System (FERS) employees may contribute up to 14 percent of their base pay, and Civil Service Retirement System (CSRS) employees may contribute up to nine percent.

For more information, call 1-877-276-9287 or go to: <https://www.abc.army.mil>.