

IN THIS ISSUE

A Message from the PEO...
Page 2

Army Vice Chief of Staff
Discusses Vehicle Fatalities,
Suicides...
Page 3

Vietnam Era Vets Honored
With Special Lapel Pin...
Page 5

Secretary of Army Bids
Farewell...
Page 9

CID Gives Tips On Protecting
Online Information...
Page 11

WORTH REPEATING

“

This is a challenging time for our nation and for our Army. My highest priority will be working to ensure Soldiers receive the necessary resources and training to remain the greatest land power in the world. I am confident our Army will fight and win wherever our nation asks, whenever our country calls.”

~ Acting Secretary
Eric K. Fanning

PEO Discusses Key Communications Obstacles in Multinational Training

By Michael S. Darnell, Stars and Stripes

Can you hear me now?

One of the biggest challenges U.S. Army Europe faces when training with allies is being able to communicate over radio systems that have incompatible encryption systems, which makes it difficult or impossible to share sensitive data.

The issue was at the forefront of discussions among top U.S. and European army officials who gathered recently at USAREUR's training grounds.

They were getting a lesson in the challenges inherent in multilateral training as allies from 13 countries are participating in Combined Resolve V, an exercise that seeks to increase cooperation between armies from across Europe.

The general officers toured American and Dutch tactical operations centers at the training grounds here to learn about the obstacles to communicating with troops in the field.

“At this moment, we are not fully interoperable with the lower level,” said Dutch Capt. Mathijs DeBruijn.

Being able to train as if it were a real battle is critical, officials said.

The major issue, DeBruijn said, is that the radios multinational units use in the field rely on a piece of technology called the tactical voice bridge. This stopgap component put into use just last year allows for radios from different nations with different encryption standards to talk to each other.

Before the voice bridge was developed, communication between two radios with different types and echelons of encryption was difficult if not downright impossible.

DeBruijn said the voice bridge works, but it has limitations. The device needs to be programmed for

the types of radios that are plugged into it, and allied forces have only limited numbers of them. Right now, the Dutch operations center only has one in use.

This means most of their most vital communications are done over an unsecured line, which further limits the type of information that can be passed between allied units.

“We will have to use just single-channel, plain text, unciphered radio. So that means we cannot



U.S. Army Photo

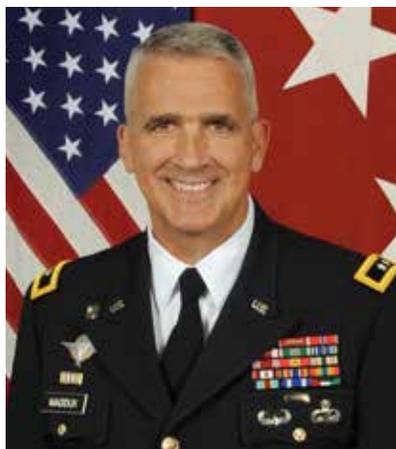
Maj. Gen. Jonathan Maddux (left), Program Executive Officer for Simulation, Training and Instrumentation answers a journalist's questions during a Multinational Interoperability Executive Site Visit at the Training Support Center's Multiple Integrated Laser Engagement System (MILES) warehouse located at the Joint Multinational Readiness Center, Hohenfels, Germany, Oct. 29, 2015. (U.S. Army photo by Visual Information Specialist Gertrud Zach).

use any classified information on that radio net,” DeBruijn said. “What would really help us, if that is possible, to connect radios directly to each other without configuring the item that’s in between.”

Maj. Gen. Jonathan Maddux, program executive officer for U.S. Army's Simulation, Training and Instrumentation, said his department plans to ask the Department of the Army to ease some restrictions on ally-to-ally communication.

continued on page 11

PROGRAM EXECUTIVE OFFICER



MG JON MADDUX

“ **PLEASE
DISCUSS THE
IMPORTANCE
OF SAFE
DRIVING WITH
ALL MEMBERS
OF YOUR FAMILY,
NOT JUST DURING
THE HOLIDAY
SEASON, BUT
THROUGHOUT
THE YEAR.**

— MG Jon Maddux

To The PEO STRI Workforce,

As we enter the new year, I want to share with you an alarming statistic released by the National Highway Traffic Safety Administration (NHTSA).

Almost 90 people on average lose their lives each day – and more than 250 are injured every hour – due to drinking and driving, not wearing a seatbelt and the many other factors associated with traffic crashes. Sadly, as mentioned in the message from Gen. Allyn, our Vice Chief of Staff, on page 3 of this newsletter, last year 83 Soldiers died in traffic accidents.

According to the NHTSA, when the clock strikes midnight to welcome in the new year on January 1, more than 35,000 Americans will not be around to welcome in the new year. That’s because they died in needless traffic accidents this year.

I say needless because 94 percent of them were from human error such as drunken, drowsy or distracted driving.

That equates to 32,900 needless deaths because the driver had consumed too much alcohol, hadn’t properly rested before getting behind the wheel or just had to send that last message.

It makes absolutely no sense in getting behind the wheel of a two-ton vehicle or on a motorcycle when you are too tired or have had too much to drink. It is so easy to be honest about your condition and pass those keys on to someone else or take a taxi. It might just save your life.

Distracted driving is also taking many lives. Statistics show that texting while driving makes drivers 23 times more likely to crash and is the same as driving after having consumed four beers. Statistics also show that texting for five seconds while driving at 55 mph is the same as driving the length of a football field blindfolded. I have no doubt that you would not knowingly do that. Why, then, would you even consider texting while driving?

Please discuss the importance of safe driving with all members of your family, not just during the holiday season, but throughout the year. Share with them some of the leading causes of traffic fatalities besides texting while driving or driving under the influence. Simple things like looking at the passing scenery, adjusting the radio or interaction with other passengers are causing needless deaths on our Nation’s roadways.

On behalf of PEO STRI’s leadership team, thank you for the excellent work you continue to do for our Soldiers on a daily basis.

Regards from your Program Executive Officer,

Army Vice Chief of Staff Urges Leaders to Focus on Safety, Suicide Prevention

By General Dan Allyn, 35th VCSA

Our Army is facing two deadly challenges that directly pose extreme risk to our Force and Readiness: driving fatalities and suicide. These challenges demand immediate and increased attention and engagement by leaders at every echelon.

Driving remains the single deadliest activity in the Army. Driving fatalities, on- and off-duty, accounted for 83 of the 112 Soldier deaths from accidents last year. Indiscipline, speeding, overconfidence, and alcohol consumption continue to be the leading factors in fatal motor vehicle accidents. Leader intervention is essential to reverse this deadly trend.

Our Army needs leaders to establish and enforce a culture that shapes how Soldiers behave, both on- and off-duty. Soldiers must understand how their actions affect their unit, and their training must reinforce the right decisions. Leadership is consistently decisive when we rigorously enforce training, discipline, and standards ... and that extends to off-duty conduct. Leaders at every echelon must undertake comprehensive reviews of our driver and motorcycle training programs, and leverage them to enforce leader follow-up on high-risk actions by our Soldiers and in our units. These are proven strategies to confront high-risk behavior through early intervention.

Another area for decisive leadership is outreach to our Soldiers and Teammates

at risk of suicide. Compared to this time last year, our Army has 29 more cases of suicide, which is a tragic and alarming trend. The health and well-being of Soldiers, Department of the Army Civilians, and Families remains our sacred responsibility.

AS LEADERS, WE ARE ENTRUSTED TO ENSURE THE READINESS AND RESILIENCE OF THOSE SERVING OUR NATION.

We must identify early warning signs and provide tools to help place a premium on leader intervention and put a spotlight on effective leader intervention. The Army offers a number of high-quality treatment programs, screenings, and resources, such as comprehensive pre- and post-deployment screenings for early identification of behavioral health conditions. Additionally, Military OneSource and the National Suicide Prevention Lifeline provide



24-hour assistance. I encourage leaders at every echelon to publicize and use these valuable resources to save lives.

Current trends in driving fatalities and suicide must be reversed. We must all recognize the needs of our Soldiers, Department of the Army Civilians, and Families and leverage all available tools to assist them in making sound choices. Every Soldier has a leader in the right position to make a difference. In our Army, no Soldier, Department of the Army Civilian, or Family member stands alone. Army leaders are decisive to mission success.

Army Strong!

Inside STRI is an authorized publication for military and civilian members of the U.S. Army Program Executive Office for Simulation, Training and Instrumentation, Orlando, Fla. 32826. *Inside STRI* is published under the authority of AR 360-1 and applies the Associated Press Stylebook industry standard. Contents of *Inside STRI* are not necessarily the official views of, or endorsed by, the U.S. Government, Department of Defense, Department of the Army, or PEO STRI. Editorial material for publication should be submitted to PEO STRI Public Affairs Office, 12350 Research Parkway, Orlando, Fla. 32826. The PAO reserves the right to edit all material submitted for publication. For more information about PEO STRI or to view *Inside STRI* online, visit our website at www.peostri.army.mil
EDITOR: Kristen Dooley McCullough, Editor-in-Chief [kristen.a.mccullough.civ@mail.mil] • DESIGN: MSB Analytics, Inc. [usarmy.orlando.peo-stri.list.cggraphics@mail.mil]

Army Chief of Staff Dispels Four Myths of Warfare

By David Bergun, Army News Service

The Army “exists for a single purpose and none other: to fight and win wars in defense of the United States of America. That’s it. Fighting and winning wars is our *raison d’être*,” Army Chief of Staff Gen. Mark A. Milley said.

Milley was keynote speaker at the Dwight David Eisenhower Luncheon, hosted by the Association of the United States Army during its annual meeting on Oct. 13.

“We are a great Army and we must remain so, but we must never forget that we are not in this fight, and never have been in this fight alone,” he said, citing the great work of the men and women of the other services and allies.

He then spoke of the myths that are out there.

DELUSIONS OF WAR

When leaders, especially those “within the beltway,” deal with budgets and figure out force structure and future investments, they retain “myths that are factually and historically incorrect,” Milley said.

Those myths can lead to bad policy choices, not only for the Army, but for the nation’s security. Those who promulgate these illusions are often those who’ve “never actually experienced the blood and the sweat and the tears of war,” he said.

The chief then discussed each of these myths, which he described as probably “an illusion of hope in the human psyche ... or perhaps sheer human incompetence.”

MYTH: WARS WILL BE SHORT

Wars of the future will be short, perhaps even “a minor dustup,” is the first myth he said.

America’s founding fathers had no intention of fighting an eight-year war against the greatest power of the day, Great Britain, he said. “Most thought they’d rebel a bit, get some tax relief and do so with their local militias.”

Americans, both in the North and South during the civil war, expected a short war. They had “no clue they’d entered a four-year bloodbath that would be the deadliest in American history,” he said.

No leaders in Europe or elsewhere in 1914 thought they’d “butcher an entire generation of their youth in the next four years ... and set conditions for World War II, the most devastating war in human history.”

Milley then cited the surprise of those who thought the wars in Korea and Vietnam would be short and with relatively few casualties.

And, “I doubt we thought we’d still be in the Balkans, Afghanistan and Iraq when we first started at the places I’ve been,” he said.

“Wars are funny things. They have a logic all of their own. And they rarely conform to preplanned timelines,” the chief said. “They’re rarely short.”

MYTH: WIN WITH TECHNOLOGY

The second myth is that wars can be won with advanced technologies,” Milley said.

Proponents of this myth say that modern weaponry can provide standoff capabilities from the air and from the sea, he said.

“Our precision munitions and cruise missiles are wonderful, and I love them. They deliver a devastating punch. But this too is very seductive,” he said.

Wars cannot be won on the cheap in terms of blood and sacrifice, he said. “Those of us who’ve seen battles up close, who’ve watched our comrades die, I deeply want that to be true. I want wars to be won from standoff ranges.”



U.S. Army Photo

Army Chief of Staff Gen. Mark A. Milley serves as keynote speaker at the Dwight David Eisenhower Luncheon during the annual meeting of the Association of the United States Army, Oct. 13, 2015

But unfortunately, it’s “fantasy,” not fact, he said. “After the shock and awe comes the march and fight.”

He cited the belief that strategic bombing during World War II could bring the war to a quick end. That didn’t happen. Soldiers on the ground won the battles.

Another example, he said, was Iwo Jima, where his father fought. Days and weeks of pounding by aircraft and battleships caused relatively few casualties and the Marines were surprised at the stiff resistance they faced when they landed, as well as the high number of their own dead and wounded that resulted.

MYTH: SPECIAL FORCES ALONE CAN WIN

The third myth, Milley said, is that special forces can do it all and America only needs an elite, rapid-reaction force to win wars of the future.

While America’s special operations forces are the best in the world, their success at killing high-value targets is a necessary tactical strategy, but not sufficient, he said.

To prevail in war takes so much more than killing high-value terrorists with drone strikes and small-unit raids, he said. Like war from standoff ranges, this myth is very seductive.

continued on page 11



Secretary of Defense Addresses Vietnam War Congressional Commemoration

As Delivered by Secretary of Defense Ash Carter, Washington, D.C., July 8, 2015

Members of Congress, distinguished guests, colleagues from the Department of Defense past and present, members of the Vietnam Commemoration Advisory Committee... thank you for being here today. Thank you to the organizers and commemorative partners of this important event, and thousands like it across the country, and the entire Vietnam commemoration effort. And, most importantly, thank you to the Vietnam-era veterans and their families who join us – you honor us with your presence.

In a year of anniversaries – for this year also marks the 150th anniversary of the end of our Civil War, the 70th anniversary of the end of World War II, the 65th anniversary of the start of the Korean War – today we gather to remember the Vietnam War, and to honor those who served in it.

We remember the 50th anniversary of President Johnson's Executive Order establishing the Vietnam Service ribbon. And we honor our 7.2 million living Vietnam-era veterans, their fallen comrades-in-arms, including those still unaccounted for, and the families of all who served.

That era's proud soldiers, sailors, airmen, Marines, and Coast Guardsmen are part of a deep line of warriors – patriots who served and fought in Lexington and Concord, at Gettysburg and Midway, at Ia Drang and Khe Sanh, and, more recently, in Fallujah and Helmand.

Some of those Vietnam veterans are here today. Some bear the wounds of war or the wear of age. Some carry with them memories of fallen comrades – American fathers, uncles, brothers, and sisters who did not make it home. And others proudly wear Vietnam Veteran lapel pins and Gold Star buttons to remember the service and sacrifice of years past.

On behalf of President Obama and the entire Department of Defense, I thank all of you for your service. I thank you for those sacrifices. And I thank you for the lessons that you've taught all of us and continue to teach us.

One of the reasons the United States has excelled is that, as a nation, we learn and innovate. And one reason why we have the finest fighting force the world has ever known, is that our military is a learning organization. We learn from successes, we learn from setbacks...we take the time to delve into our experiences and always strive to do better.

The Vietnam War taught us many lessons – many hard-won, some difficult to swallow – but all of them have made us a better country and a better military. And there are two that I believe are particularly important to remember this day.

First, we leave no one behind. We are not the only military with that ethos, nor are we the only nation with a POW/MIA accounting effort. But there are few that have such a steadfast and sustained commitment, which is about more than raising the iconic POW/MIA symbol up on flag poles around the nation.

It's about the promise we make and we work hard to keep.

Thanks in part to the staunch advocacy of Vietnam veterans and POW/MIA families, the Department of Defense has over 650 people devoted to accounting for the missing and searching for, recovering and identifying their remains, including the 1,627 still missing from the Vietnam War. I saw some of that continuing effort on my trip to Hanoi last month where I visited one of our POW/MIA accounting offices.

The second lesson is that we must support our warriors, regardless of our feelings about the war. Unfortunately that was a lesson some learned the hard way in the Vietnam-era. But I am pleased by – and again, we have many Vietnam-era veterans to thank for it – the support for today's veterans and servicemembers, including the post-9/11 GI Bill, and how our troops today are welcomed home. And I want to take this opportunity to thank you, our Vietnam-era veterans, for that lesson, and to again welcome all of you home.

Vietnam-era veterans and their families helped America learn those lessons...and ensure we will never forget them. Some do so quietly, mentoring today's men and women in uniform or traveling to airports to welcome home those returning from the wars in Afghanistan and Iraq. Some do so more publicly, continuing their service in government offices in this Capitol, elsewhere in Washington, and across the country, including my colleagues Secretary John Kerry, and Senator John McCain.

Thank you again to all the Vietnam-era veterans here and around the country. May God bless you and your families for years to come.



PEO STRI's Threat Systems Management Office Plays Major Role in Cyber Exercise

By Claire Heining, U.S. Army

Imagine taking a test and not learning the results until three or four months later. It's a long time to wait before knowing what you need to work on to improve.

But that's how the Soldiers responsible for cyber network defense at the Army's Network Integration Evaluations (NIEs) typically measured their performance – through a report governed by formal programmatic test constraints.

Now, spurred by the rising prominence of cyber warfare and changes to the NIE construct, those Soldiers are teaming with mock hackers to get feedback in real time. It's one of several cybersecurity process improvements made possible by the Army's recent shift to holding one annual NIE and one annual Army Warfighting Assessment (AWA) – a new event featuring Soldier-led evaluations of concepts and capabilities, but without formal system tests for record.

“Instead of saying, ‘you didn't catch this, we'll let you know more in a report that comes out three to four months later,’ we had our cyber network defenders sit down with the Red Team every three days,” said Chief Warrant Officer 3 Greg Olivo, cyber information protection technician for the Brigade Modernization Command, known as the BMC. “It was open book both ways, so I think it was a great learning session for the cyber network defenders and for the Red Team as well. The beauty of this is they'll get a lot smarter – they'll use the lessons learned during AWA to apply to an NIE.”

The cyber Soldiers' interaction with the Red Team – a group of trained hackers from the U.S. Army Threat Systems Management Office – occurred throughout NIE 16.1, which took place at Fort Bliss, Texas, and White Sands Missile Range, N.M., in September and October and was the final proof-of-concept for the AWAs, which formally begin in the fall of 2016. More than 12,000 U.S. Soldiers and 1,140 coalition personnel took part in the exercise, which



Photo by Dave Vergun, ARNEWS

Soldiers defend the network and analyze intelligence at 2nd Armored Brigade Combat Team, 1st Armored Division's brigade headquarters and tactical operations center at Fort Bliss, Texas, during Network Integration Evaluation 16.1, the final proof of concept for the Army Warfighting Assessment (AWA).

evaluated 78 different concepts and capabilities through realistic operational scenarios and a formidable opposing force (OPFOR).

“Cyber defense is my major concern – we're facing a nation-state actor when it comes to cyber defense,” said Col. Chuck Masaracchia, commander of 2nd Armored Brigade Combat Team, 1st Armored Division, the main operational unit that executes the NIEs and AWAs. “The greatest threat that I face as a brigade commander on the battlefield is not tanks, Bradleys, snipers or IEDs [improvised explosive devices], it's the threat to computer network operations.”

AN EXPERIMENTAL ENVIRONMENT

Going forward, the Army plans to execute one NIE per year, focused on meeting integrated program of record test requirements, and one AWA per year, which will provide a more experimental environment to help shape requirements, with an emphasis on joint and coalition interoperability. The AWA will also allow the Army to improve its cyber posture by expanding training opportunities, developing system-of-systems level standard operating procedures and refining unit tactics, techniques and procedures.

continued on page 11



Cybersecurity Awareness Month Bolsters Ways Army Can 'Stay Protected While Connected'

By U.S. Army Cyber Command

In recent months, headlines about cybersecurity incidents have captured national attention. From the Office of Personnel Management to the Sony Pictures intrusion, it has become clear that a single cyber intrusion can affect large numbers of people and cost millions of dollars in damage.

While these incidents garnered significant media attention, they represent a very small piece of a much larger picture, akin to individual pixels in a high-resolution image.

"It only takes one careless or malicious act anywhere on our networks to threaten Army operations," said Lt. Gen. Edward C. Cardon, commander of Army Cyber Command and Second Army.

There are two assumptions the Army operates on each day: networks will become more and more vital to operations, and networks and the systems on those networks are constantly at risk.

To help stem the tide of malicious acts by hackers, non-state actors, nation states and insider threats, the Army must be able to count on a third assumption: individual users will remain vigilant when operating on Army networks. That's why the Army's third Cybersecurity Awareness Month observance this month focuses on risk management at the user level, the first line of defense against attacks in cyberspace.

"Cybersecurity is everyone's mission," Cardon said. "Most vulnerabilities and malicious acts against Army systems could be prevented by following and enforcing cybersecurity standards and policies."

The 2015 theme, "Stay Protected While Connected," stresses that vigilance and good online habits by individuals and organizations are critical to keeping Army networks, information and personnel safe.

Beyond educating the workforce, the Army has chosen Cybersecurity Awareness Month to launch a requirement tasking organizations to develop plans that integrate cybersecurity

risk assessment, management and mitigation into all phases of operations.

"This year the Army will focus on the measures all commanders, leaders and supervisors must understand to assess and manage risk, as well as techniques to effectively and continuously monitor people, processes and technologies necessary to identify, evaluate and respond to insider threats," wrote Army Secretary John M. McHugh in a memorandum outlining the priorities of this year's observance.

Those plans, measures and techniques include identifying and routinely reviewing the status of privileged users and ensuring they meet all access requirements; assessing personnel for insider threat indicators; minimizing system administrative privileges; completing necessary training; developing processes to monitor user accounts and

activities and control access; identifying sensitive information the organization creates or handles and certifying that it is properly protected; ensuring that personnel and physical security measures to safeguard systems are adequate, and promoting a culture that embraces the belief that online misconduct is not in keeping with the Army values.

"The Army must create a culture of awareness at every echelon," McHugh wrote. "Proactive measures can help the Army safeguard the integrity of Army networks and systems, and protect information and personal data."

ABOUT US: Army Cyber Command and Second Army directs and conducts cyberspace and information operations as authorized or directed, to ensure freedom of action in and through cyberspace, and to deny the same to our adversaries.



Soldiers practice proper online security precautions while performing their duties.

U.S. Army Photo





Mr. Eric Fanning

Acting Secretary of the United States Army



Mr. Eric K. Fanning was appointed Acting Secretary of the Army by President Obama on November 3, 2015.

As Secretary of the Army, he has statutory responsibility for all matters relating to the United States Army: manpower, personnel, reserve affairs, installations, environmental issues, weapons systems and equipment acquisition, communications, and financial management.

He was previously appointed Acting Under Secretary of the Army and Chief Management Officer by President Obama on June 30, 2015. He served as the Secretary of the Army's senior civilian assistant and principal adviser on matters related to the management and operation of the Army, including development and integration of the Army Program and Budget. As Chief Management Officer (CMO) of the Army, he advised the Secretary on the effective and efficient organization of the Army's business operations and initiatives for the business transformation of the Army.

Mr. Fanning previously served as The Special Assistant to the Secretary and Deputy Secretary of Defense. He helped manage Secretary of Defense Carter's transition, built his leadership team, and oversaw the day-to-day staff activities of the Office of the Secretary of Defense.

From April, 2013 until February, 2015, he served as the 24th Under Secretary of the Air Force. As Under Secretary and Chief Management Officer of the Air Force, he oversaw an annual budget of more than \$110 billion by serving as co-chair of the top Air Force corporate decision making body, the Air Force Council, and also led the Air Force Space Board, the Air Force Energy Council, the Force Management and Development Council, and numerous other Air Force decision-making bodies.

From June, 2013 through December, 2013 Mr. Fanning served as Acting Secretary of the Air Force.

From 2009 to 2013, he served as the Deputy Under Secretary of the Navy/Deputy Chief Management Officer. In this role, he led the department's business transformation and governance processes and coordinated several efforts to identify enterprise-wide efficiencies.

From 2008 to 2009, Mr. Fanning was Deputy Director of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, which issued its report in December of 2008. He joined the commission staff from CMG, a strategic communications firm, where he was managing director. From 2001 to 2006, Mr. Fanning was Senior Vice President for Strategic Development at Business Executives for National Security, a Washington, DC-based think tank, where he was in charge of international programs and all regional office operations in six cities across the country. He traveled to more than 30 countries, mostly in Africa, the Middle East and Europe, including multiple trips to Iraq and Afghanistan.

Prior to joining BENS, Mr. Fanning was at Robinson, Lerer & Montgomery, another strategic communications firm. From 1997 to 1998, he worked on the national and foreign assignment desks at CBS National News in New York. From 1991 to 1996, he worked in various political positions in Washington, D.C.: he was a research assistant with the House Armed Services Committee, a special assistant in the Immediate Office of the Secretary of Defense, and Associate Director of Political Affairs at the White House.

Mr. Fanning is a graduate of Dartmouth College.



SECRETARY OF THE ARMY
WASHINGTON

To the Soldiers, Civilians and Families of our Army:

Serving as your Secretary for these past six years has been the honor of my life and—by far—the most fulfilling experience of my professional career.

While many days have certainly been long, the years have been amazingly short because my time here has been so very rich and rewarding. Without question, that is thanks to all of you: the men and women that I have been privileged to call my teammates.

I want you to know that I have an unceasing admiration for your remarkable sense of duty and devotion. The past 14 years of war have been long and painful for our total force, your families and our Nation. But your collective strength, courage and leadership – together with your compassion and commitment – have helped America endure in the face of hardship. You are men and women of character. Trusted professionals. You always do your very best, and have committed your lives to something greater than yourselves.

Gen. Creighton Abrams once said: "There must be, within our Army, a sense of purpose and a dedication to that purpose. There must be a willingness to march a little farther, to carry a heavier load, to step out into the darkness and the unknown for the safety and well-being of others." I could not agree more. Over the past six years – indeed for as long as I been involved with Army matters – you have shown me such sense of purpose and such dedication day in and day out.

Together, you are America's indispensable Army. You are part of the rock – the foundation – that holds our great country together. You have shared uncommon lives and challenges and have done what your country has required of you. You have, quite simply, ensured our way of life. I am proud to have served in your gallant company.

I ask that you continue to accept the trust that America bestows upon you and the challenges which it carries. Continue to be the standard bearers of our noble Profession of Arms. The American people are counting on you and I know that you will not let them down.

Thank you, thank you, thank you for who you are and what you do. All of you.

God bless you, God bless your families, and God bless this great and glorious Army that keeps us free. Army strong!

Criminal Investigation Command Gives Tips on Protecting Online Personal Information

By U.S. Army Criminal Investigation Command

As a result of recent world events and a continual effort to protect the force, special agents with the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit are strongly recommending that anyone affiliated with the U.S. military, review their social media accounts to make sure they are using the best security settings to protect their online profiles.

Social media platforms such as Facebook, Twitter and LinkedIn are powerful tools that can help bring communities together. However, an individual's online profile can provide cyber criminals with an endless pool of personal information and potential targets to be exploited. As such, it is vital that individuals stay on the alert and be personally responsible for their online presence to protect themselves, their loved ones and the Army.

With that in mind, CID is providing the following information to help the greater Army community protect themselves online and significantly reduce the chance of becoming a victim of cyber crime.

SOCIAL NETWORKING SAFETY TIPS: THINGS TO KNOW

* The internet does not forget. Once something is posted on a social networking website it can spread quickly, and no amount of effort can delete it. Do not post anything you would be embarrassed to see on the evening news.

* You are not anonymous. Cyber criminals have the capability to gather and exploit both individuals and organizations if the information is out there.

* More isn't always better. Participating in multiple social networking sites significantly increases a person's risk, and affords cyber criminal alternate avenues to strike and gather information.

HOW TO PROTECT YOURSELF:

* Know the terms on social networking websites. Facebook, Twitter, LinkedIn and other social networking sites frequently change their privacy and user policies. Social networking sites privacy settings default to everyone. This means anyone, can view your

profile, not just the people you know. Securely configuring one's account will minimize who can see your information.

* Safe social networking. Never disclose private information when using social networking websites. Be very selective who you invite or accept invitations from as criminals often use false or spoofed profiles to gain access to personal and private information, such as birthdates, marital status, and photographs. Social media posts that contain personal identifying information (PII), digital photos that contain metadata (i.e., information written into the digital photo file such as who owns it, contact information, location, and internet search terms) can be used against you and your family.



* Click with caution. Always use caution when clicking on links in social networking posts, even from someone you know. Reports of personal social networking accounts being hacked by criminals have increased in recent years. Clicking on a link that appears to be benign in nature may in fact contain embedded malware that can compromise your device. Once compromised, any data on your device can be exploited.

* Hide your profile from search engines. This can be accomplished by going to the social networking site account settings and unchecking the "Public Search Results" box. This will remove your public preview from Google, Bing, and Yahoo search returns.

* Check-out and tag-out. Do not use check-ins or post your specific location on social

media. Also, prevent people from "tagging" you in photos and videos.

* Login No No's. Do not use your social networking site to login to other sites or use the save password, remember me, and keep me logged in options from a public or shared device. Use strong, unique passwords and never use the same password for all online accounts.

* Install/Update your anti-virus/firewall software. Antivirus and firewall software is a must for anyone to safely navigate online. Always keep your security software up to date in order to provide the most complete protection from malicious programs as thousands of new viruses are detected every year. Also, ensure your antivirus software program updates automatically and scans your computer on a recurring schedule.

As a service to the U.S. Army and DOD communities, the Computer Crime Investigative Unit has produced comprehensive how-to guides to safely configure an individual's Facebook and Twitter accounts. Configuration guides for other social networking platforms will be available in the near future.

To download the guide, visit <http://www.cid.army.mil/documents/CCIU/2can/SocialNetworkingSafetyTips.pdf> and select the respective guide at the bottom of page one.

Additional information about computer safety and cyber related crimes can be found on the U.S. Army Criminal Investigation Command's CCIU webpage at <http://www.cid.army.mil/cciu.html>. Simply select the Cyber Crimes Advisories on the left side of the page to review previous cyber crime alert notices and prevention flyers.

CID strongly recommends that Soldiers, civilians and family members who have information of any known crime committed by a Soldier, a crime that occurred on their respective post, camp or station, or is a victim of a crime to contact their local CID office, dial 1-844-ARMY-CID (844-276-9243) or email CID at Army.CID.Crime.Tips@mail.mil.

“The protocols, the encryption, the demodulation, the translators ... all that needs to be looked at and addressed if we’re going to train as we fight,” he said.

Maddux disclosed that the Army is collecting data ahead of a potential MILES equipment upgrade, both for Americans and the partner nations exercising with USAREUR. The MILES — or Multiple Integrated Laser Engagement System — is equipment American forces use to simulate combat between friendly units. Other partner nations have similar equipment, but there are differences.

“Now our weapons systems are different than some of our coalition partner weapons’ systems, so therefore we know that there’s gaps that exist there,” Maddux said. To minimize those gaps, his department is looking at software and calibration upgrades to the MILES gear in order “to have engagements that are accurate on both ends.”

As with all things, he said, the need for upgraded capabilities in communications and simulated warfare has to be balanced against a USAREUR budget that continues to shrink.

“It’s important that we get it right and prioritize those tasks so we can have the big Army take a look at those and consider those as we compete in this fiscally constrained environment,” he said.

PEO STRI'S THREAT SYSTEMS MANAGEMENT OFFICE PLAYS MAJOR ROLE IN CYBER EXERCISE *continued from page 6*

“For an NIE the focus is correct – the focus should be evaluating the system that the Army is thinking about purchasing,” Olivo said. “But for AWA, we’re working to strike a balance to make sure whatever system we’re evaluating is set up correctly and doesn’t have vulnerabilities, while at the same time training our cyber security team.”

For past NIEs, the Threat Systems Management Office (TSMO) Red Team’s mission was to provide each system under test a focused cyber-threat evaluation, which involved very little cooperative interaction with network defenders during the event, said Chip Wurslin and Robert Wedgeworth, the TSMO Cyber OPFOR co-leads for NIE and AWA.

But for NIE 16.1, as the AWA proof-of-concept, the Army devised and implemented a training plan that emphasized iterative and open communications between cyber OPFOR operators and network defenders. Prior to the exercise, the cyber Soldiers were informed of approximately 20 focus areas that would make up their cyber “report card” at the conclusion of the event – part of a new evaluation rubric designed to quantitatively assess network defenders’ ability to detect and mitigate simulated threats.

But they also had the opportunity to improve as they went along. For example, when the cyber network defenders learned they had failed to detect a certain type of malicious activity on the network, they asked the Red Team to deploy similar traffic within the next few days, to see if they could stop it once they were aware of that mode of threat.

“They were not only able to catch malicious traffic, but to change their thinking,” Olivo said.

One defender even commented “that he had learned more about defending against Cyber OPFOR effects from this single event than during all previous NIEs combined,” Wurslin said. “The evaluation results allowed defenders to focus on areas requiring more attention and helped to better prepare them for follow-on NIE events.”

MYTH: ARMIES EASY TO REGENERATE

If the Army is too small for the conflict at hand, the fourth myth is that one simply needs to recruit a large number and put them through basic training, Milley said, and “presto, you have a unit.”

The reality, though, is much more challenging, he said. Leaders take many years to develop the competencies and skills necessary to wage ground combat.

A platoon sergeant will take 10 to 15 years while a battalion commander will require 15 to 17 years, he said. Today’s weapons systems likewise take a long time to master, especially involving joint and combined fires.

COST OF MYTHS

The cost of these myths have resulted in the loss of thousands of lives throughout American history, Milley said, acknowledging that he lives with the “ghosts of our battles past.

“For me, that number is 241,” he said. “We see their faces and all of them speak to us from the grave.”

As chief of staff, he said he promised to make the Army the best equipped and trained as he can to minimize the loss of life and win. “Those ghosts remind us that no Soldier should ever die because they were not ready.”

SECURITY AND SPEED

The Red Team collaboration was one of several changes the Army is implementing for NIE and AWA to improve Soldiers’ and systems’ security posture. While NIE for several years has been the Army’s premier venue for Soldier-led operational evaluations of tactical communications systems, the process has traditionally focused on speed rather than security.

“The NIE is set up to get things working right away – not to get them working securely right away,” said Col. Bryan J. Stephens, Cyber Focal director for the Assistant Secretary of the Army (Acquisition, Logistics and Technology), System of Systems Engineering and Integration (SoSE&I) Directorate. “We are now putting the processes in place to do both.”

For example, the Cyber Focal worked with Blue Team network defense personnel from the Army Research Laboratory and the 1st Information Operations Command on several steps to formalize and smooth the transition from lab-based risk reduction activities at Aberdeen Proving Ground, Md., to field operations at Fort Bliss. This synchronization ensured that systems’ cyber vulnerabilities discovered in a lab setting could be mitigated prior to the start of NIE 16.1. Based on the results, SoSE&I is now implementing a tracking mechanism that will allow NIE and AWA participants to monitor Blue Team findings across past and current events, so the Army can better address consistent cyber trends.

Additionally, to boost security in the AWAs’ coalition network environment, SoSE&I is extending by two weeks the Validation Exercise phase that takes place prior to the start of field operations. The extra time to verify that systems are properly configured and secured will reduce cyber risk for U.S. and partner nation units, while again providing better training opportunities for cyber Soldiers.

“Cybersecurity is a team sport, and if one team member is a weak link, the entire team suffers,” Stephens said. “With these changes to NIE and AWA, the Army can truly work as a team to improve our collective cyber defense.”

PEO STRI PARTICIPATES IN ANNUAL CONFERENCE



U.S. Army photo

Maj. Gen. Jon Maddux, PEO STRI's program executive officer, speaks with Congressman John Mica during the annual conference.



U.S. Army photo

Maj. Gen. Jon Maddux, PEO STRI's program executive officer, greets Congressman Bobby Scott at the annual conference.



U.S. Army photo

Col. Vince Malone, PM TRADE, briefs the audience during the Training and Simulation Industry Symposium.



U.S. Army photo

Ms. Chérie Smith, deputy program executive officer, greets Congressman Bobby Scott while Congressman John Mica looks on.



U.S. Army photo

Jerry Sirmans, deputy project manager, ITE, gives the invocation at the opening ceremonies.



U.S. Army photo

Lt. Gen. Michael Williamson, ASA(ALT)'s principal military deputy, is briefed by Col. Daniel Irizarry, clinical advisor, Joint Program Office for Medical Modeling and Simulation, while Maj. Gen. Jon Maddux, PEO STRI's program executive officer looks on.



U.S. Army photo

Rob Wolf (white shirt), PM TRADE, briefs Congressman Bobby Scott (left) and Congressman John Mica (right) on the Squad Overmatch Study during the annual conference.



U.S. Army photo

Col. Bill Canaley, director Field Operations, briefs Maj. Gen. Jon Maddux, PEO STRI's program executive officer, during the Interservice/Industry Training, Simulation and Education Conference.



U.S. Army photo

Lt. Gen. Michael Williamson, ASA(ALT)'s principal military deputy, briefs the audience during the General Officer Panel portion of the Interservice/Industry Training, Simulation and Education Conference.

PEO STRI EMPLOYEES REACH MILESTONE CAREER SERVICE MARKS



25 YEARS | HARROLL INGRAM
PM TRADE



25 YEARS | TRACY STEPHENS
G8



25 YEARS | PERCY PARKER
FIELD OPS



25 YEARS | MIKE WANKLYN
PM ITE

During the December Town Hall, Maj. Gen. Jon Maddux, program executive officer, presented certificates to

PEO STRI employees who have reached the 25 years or higher career service mark. Pictured are those employees who have served for 25 years or more.



30 YEARS | LIBBY DEVINE
G2



30 YEARS | JOHN KIRCH
Special Staff



30 YEARS | ROBERT DIXON
PM ITTS



30 YEARS | INGRID NEAL
FIELD OPS



30 YEARS | PETE WALTON
PM TRADE

STRI IN FOCUS



U.S. Army Photo

Maj. Gen. Jon Maddux, program executive officer (left), and Sgt. Maj. Alan Higgs, PEO STRI's senior enlisted advisor (far right), pose with the honor guard during the Assistant Secretary of the Army for Acquisition, Logistics and Technology's Awards Banquet on Dec. 4.



U.S. Army Photo

Michael Kilcrease, whose duty station is Fort Rucker, Alabama, was named as the Employee of the Quarter for the fourth quarter of fiscal year 2015.



U.S. Army Photo

Maj. Gen. Jon Maddux, PEO STRI's program executive officer, presents the Commander's Award for Civilian Service to Scott Pulford, G3, during the December Town Hall Meeting.



U.S. Army Photo

The Small Unmanned Aerial Systems Team, PM ITTS, poses for a photo at their duty station in Redstone Arsenal, Alabama prior to winning Team of the Quarter honors for the fourth quarter of fiscal year 2015. From left are Michael Francis, Cheryl Grant, Mya Willis and James Story.



U.S. Army Photo

Maj. Gen. Jon Maddux, PEO STRI's program executive officer, presents the Commander's Award for Civilian Service to Devin Lyders, Deputy G3, during the December Town Hall Meeting.



U.S. Army Photo

Mr. Joe Giunta, executive director, Army Contracting Command – Orlando, presents the Meritorious Service Medal to Maj. Guillermo Santiago during the major's retirement ceremony held on Dec. 11.



U.S. Army Photo by Spc. Von Marie Donato, Public Affairs Specialist, 3rd Armored Brigade Combat Team, 1st AD

Maj. Gen. Jon Maddux, PEO STRI's program executive officer, attends a briefing at Bold Quest 2015 hosted at the Fort Bliss Simulation Center in El Paso, Texas Oct. 6. Bold Quest is a U.S. joint staff-sponsored coalition capability demonstration and assessment series to improve interoperability and information sharing across a range of coalition war-fighting capabilities with partner nations.



U.S. Army Photo

PEO STRI employees who served a mentors during a Disabilities Mentoring Day sponsored by PEO STRI's Equal Employment Office on Oct. 21. The event was part of the recognition of Disabilities Employment Awareness Month.



Photo courtesy of Facebook/Office of Congressman John Mica

U.S. Congressman John Mica of Florida hosted Maj. Gen. Jon Maddux on Capitol Hill Oct. 21 to update congressional members and key staffers about PEO STRI.



U.S. Army photo

Nineteen PEO STRI employees render honor to the colors during the colors ceremony on Nov. 19 prior to being pinned by Col. Vince Malone, PM TRADE, with a commemorative lapel pin acknowledging them for their service during the Vietnam Era.



Photo by Julie A. Gaytan

Maj. Charles Seaberry, assistant program manager, Games for Training, poses with George Long (left), commander of the city of Celebration's veterans club and Gary Garofalo, chaplain of the club prior while serving as the keynote speaker during the city's Veterans Day celebration Nov. 14.



Photo courtesy of the city of Orlando

Maj. Gen. Jon Maddux, PEO STRI's program executive officer, renders a salute along with other reviewing officers at the city of Orlando's Veterans Day Parade on Nov. 14.

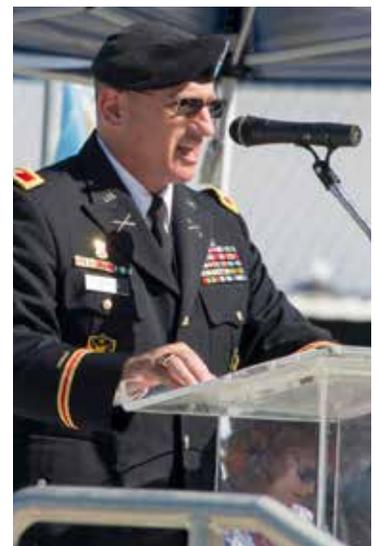


Photo courtesy of Seminole County

Col. Bill Canaley, director, Field Operations, addresses the audience as the keynote speaker at the city of Sanford's Veterans Day celebration on Nov. 11.

YOU'RE INVITED!

PEO STRI Presents

The All Saints Ball

Saturday February 27th 2016, 6:00pm
The Westin, 2974 International Pkwy, Lake Mary

Enjoy an evening with great food, comradery, dancing,
and recognition of outstanding employee contributions to the Army Branch missions

Military Attire:
Class A or Mess Dress
Civilian Attire:
Black Tie Optional

Three course dinner
Fantastic music
and entertainment

Cash or Checks payable to
'Parks and Recreation'

Discounted \$ 94
Hotel Group Rate
For Room Reservations
(407) 531-3555

Submit payments to
Respective Project Manager
Executive Assistants or
PM Representative

For further information
Major Robert Crapanzano
robert.a.crapanzano.mil
@ mail.mil

Military Members, Government Employees, and Support Contractors
\$55 per person

Chicken or Fish
Dinner Selection

Awards will be presented during the evening

Army DOES Beat Navy, With Help from the Air Force

While the annual Army – Navy football game hasn't gone too well for the Army Black Knights for the past 13 years, a group of PEO STRI employees along with teammates from the Air Force took to the soccer field in Orlando on November 5 and got a little revenge, beating the Navy and Marine team 2 - 0 in their annual soccer match.

The winning team members were Marco Mayor, Terese Muzio, Glynn Vincent, Julia Russell, Brian Serra, Billy Jensen, Erick Serrano, Chris Camp, Donny Clayton, Rick Copeland, Bob Wolfinger, Michel Berry, Phil Davis, Andrew Bannister, Anthony Bannister, Jean Paul, and Jose Cardena.



Phil Davis, with the Army/Air Force team, puts the ball back in play.



Brian Serra (Army shirt) and Marco Mayor (grey shirt) charge the Navy player.