

The Eagle

Published for the men and women of the U.S. Army Space and Missile Defense Command

November 2001

News Bits

AUSA to host December Space and Missile Defense Symposium in El Paso

The Association of the United States Army, in cooperation with the U.S. Army Space and Missile Defense Command, will sponsor an unclassified symposium Dec. 4-6. "Supporting Rapid Decisive Operations" will be the theme for the symposium, which will be held at the Judson F. Williams Convention Center, in El Paso, Texas.

Rapid Decisive Operations is an intergrating concept oriented at a high end, small-scale contingency in 2015 encompassing the 21st century challenges outlined in Joint Vision 2020.

The key roles of missile defense and Space in the Objective Force, as well as other related topics, will be explored in individual presentations and panel discussions.

The pre-conference registration cutoff date is Nov. 16. Registrations received after that may not be processed in advance. On-site registrations will be available. Individuals may pre-register on-line at www.ausa.org.

Hoaxes no 'Trick or Treat'

SMDC employees are reminded that anthrax hoaxes using powdery substances are not just simple pranks. The Attorney General has made it clear that such hoaxes may in themselves be criminal in nature. SMDC policy is clearly intended to protect employees in the workplace. Hoaxes are not funny; they are disruptive and contrary to the goodwill that should exist among employees and will be severely dealt with.



Photo by Jonathan Pierce

Brigadier General (P) John Urias talks to SMDC employees and their spouses in Huntsville during Security Awareness Day. He was backed by a panel of intelligence, security, and safety specialists.

Security Awareness Day addresses employee concerns

September 11th was disastrous for the families of the more than 5,000 people who lost their lives or sustained injuries due to the terrorist attack. It has also affected our economy, many reservists have been called up, and the nation has sent its Armed Forces into harm's way to eradicate this threat to our way of life.

In a practical sense, the results of Sept. 11 are most apparent to SMDC employees when we arrive for work each day. Concrete barriers offer a concrete, visible statement for all to see—we are vigilant, we are watching, our security measures have increased.

Our security measures, whatever they may be in Arlington, Huntsville, Colorado Springs, or on Kwajalein, or anywhere else, cover us like a blanket. Blankets don't eliminate the cold; they just make us warmer and better able to cope with our environment. So it is with our security measures; they don't

eliminate the threat, they just make it possible for us to cope with our environment.

Security Awareness Day activities across the command provided an enormous amount of information, and much of it is posted to the CommandNet. Meetings ranged from an ARSPACE Coffee for nearly 30 spouses to briefings held in a Huntsville convention center for more than 1,500 employees and spouses.

Awareness of our environment—in the workplace, when travelling or commuting, in the community, and at home—was the theme of every speaker.

But, a second message, no less nor no more significant, also came across. 'Let us get on with life.' Be vigilant, keep our chins up, and neither let fear intimidate us nor become the driving factor in our lives.

Jonathan Pierce
Editor



Happy Thanksgiving



Command Editorials

Vigilance needed in war against evil forces



Lt. Gen. Joseph M. Cosumano, Jr.

This month, I want to talk to you about two important subjects in connection with OPERATION ENDURING FREEDOM: what it means to be a veteran and why we need to be vigilant in protecting the force.

November 11th is Veteran's Day. Originally designated to mark the 11th hour of the 11th day of the 11th month signaling the end of World War I, Veterans' Day has evolved to commemorate the service of all our Nation's veterans.

We honor all of them, because each one took an oath to defend our country and its Constitution. As such, at any time they were ready to risk their lives to defend our country's interests at home or abroad.

As our history shows, each time they

were needed our veterans answered the call with courage, sacrifice, and honor.

And each time, the threat has been different, requiring a new response. To their credit, our Nation's leaders and our veterans have shown a great capacity for adapting to changing circumstances and having the vision to find a way to prevail over different enemies.

That said, perhaps never before has there been a greater need to adapt to what is a new kind of war than in our current struggle against terrorism.

Here, we are not dealing with nation states. Rather we are dealing with an invisible, non-nation "state" spread across many countries.

We will need to win on many levels to truly eradicate this cancer. It will not only require the courage and ingenuity of our warfighters, but the will power of the American public to endure what could be a long struggle with considerable hardship.

We will also have to win the hearts and minds of the people in the areas where terrorism breeds, showing them

what we already know, that there is no comparison between choosing a philosophy of murder and terror versus one of freedom and democracy.

Finally, our country must be vigilant in protecting its assets, including its people, infrastructure, environment and defense forces.

At Space and Missile Defense Command, our mission is to defend the United States, and every member of this command is part of that defense. Each of us has a place in the protective barrier that stands between us and the terrorists, because, as we have seen with recent events, we are only as strong as our weakest link.

To that end, all SMDC employees should give special attention to the guidance issued periodically on anti-terrorist force protection and operational security.

We are locked in a major struggle against the forces of evil, but I am confident we will prevail, especially if we are vigilant in maintaining that protective barrier of security.

What We Think

The Eagle asks: *How comfortable are you with the Commands efforts to improve workplace security?*

I am not 100 percent comfortable. I think improvements could be made in having actual drills and see how we would react. For instance, have a fake bomb in the building. How would the guards react? Are they really trained? How fast can we get out of the building? Once we pass those kinds of tests with flying colors, my comfort level would increase.



Melva Tillar ARSPACE Legal Office

I am real happy with the security that SMDC has in place. It works because when you enter the building everyone is checked twice and no one can enter an SMDC facility without proper identification. Mostly, our mail is hand-carried and most of that mail and paperwork is internal and for the most part everyone knows each other.



Linwood Gray Arlington DCSPER

Since the terrorist attack, Sept. 11, security at SMDC has been heightened. Initially, I was concerned because SMDC is not located on an installation; however, the extra safety measures (i.e., checkpoints, barriers, extra guards) have been comforting and I believe that the command is doing everything possible to protect the personnel.



Debbie Mitchell Huntsville DCSSPA

I am very comfortable. The Security and Safety Awareness Day answered several questions we have all had about SMDC security.



Debbie Christoff Arlington RM

I'm comfortable with the effort given the physical security steps that have been taken; such as the gate barriers, guards and the boulders. Nothing is completely safe, but I think an adequate attempt has been made. But nothing is going to secure you from something dropped on you if it is gas, biological or chemical.



William McQueen ARSPACE Supply

I am fairly comfortable with the measures that have been taken for the security of our personnel. They've got guards out at the gates checking ID badges and cards. As the security levels go up or down, they either increase or relax measures, so all in all I'm pretty happy with it.



Sgt. 1st Class Robert Hallam ARSPACE 1st Space Bn

The Eagle ... is an authorized unofficial newspaper published for military and civilian members of the U.S. Army Space and Missile Defense Command published under the authority of AR 360-1. The editorial style applies the industry standard Associated Press Stylebook. Contents of The Eagle are not necessarily official views of, or endorsed by, the U.S. Government, Department of Defense, Department of the Army, or U.S. Army Space and Missile Defense Command (SMDC). This monthly newspaper uses offset reproduction and has a circulation of 3,600. Reader input is solicited and welcomed; however, no payment will be made for such contributions. Please direct letters and comments to:

U.S. Army Space and Missile Defense Command
ATTN: Editor, The Eagle, P.O. Box 1500,
Huntsville, AL 35807-3801
Phone (256)955-1641 (DSN 645-1641) FAX: 645-1214
e-mail: Eagle Editor@smdc.army.mil

Publisher.....Lt. Gen. Joseph M. Cosumano, Jr.
Chief, Public Affairs.....William M. Congo
Editor.....Jonathan W. Pierce

Volume 8, Number 8



Cyber attacks on SMDC computers

by Dan Coberly
Huntsville, Ala.

While many people look toward heaven for Space and missile defense, other people look at the Internet for ways to defend cyberspace.

Pesky little parasites called viruses and worms have long plagued mankind, but only since 1981 have they eaten their way into computers. Some of the more recent electronic mutations don't even need a human host to spread. Like proverbial storks delivering a new baby, they simply locate an address file and e-mail themselves on to a new parent. More than just a nasty nuisance, computer bugs can literally kill your personal computer, freeze servers, and otherwise cost billions of dollars in economic damage.

They suddenly appear like a thief in the night, seeking to steal whatever's in sight. Quietly lurking in the background, they spread quickly like malicious gossip or a common cold. To computer users, they are a plague infecting the Internet.

Computer cancers also spread rapidly. A few weeks ago, one e-mail attachment threatened to slow down servers everywhere, prompting loudspeaker announcements at SMDC in Huntsville, warning workers to avoid opening the "as you requested" attachment. Prior to that, on July 19th, news media reported that the Code Red worm virus affected more than 250,000 Web servers worldwide in just nine hours, causing more than \$2 billion in economic damage. Soon after, a new mutant e-mail worm called "Peachy" was detected.

Peachy is meaner than most worms. Similar to the "as you requested" attachment, it can, for the first time, corrupt the contents of a computer by using Adobe document files (PDFs). The worm imbeds itself in a PDF file sent as an attachment through Microsoft's Outlook address book. Peachy is still cloning itself somewhere in cyberspace.

While government agencies are often stereotyped as slow-moving, computer security is one area where the government moves very fast. So fast, in fact, that federal employees now have a defacto new benefit: advance warnings about nasty new computer viruses in the work place before they hear it on the news and before they turn on their pristine computer at home.

If there were a Nobel Prize for heading off hackers, developing electronic vaccines, or for establishing planned parenthood among computer parasites, SMDC's computer security experts would surely have one. Thanks to their constant vigil and preemptive efforts, electronic damage is averted daily at SMDC. The unsung people at Information Management are quite adept



at diagnosing and fixing computer ailments and thwarting "hack attacks."

"My staff and support contractor teams quickly ensured that the Code Red virus patch was installed prior to any outbreak," said Bob Connell, (DCSIM). "Fact is, our internal SMDC systems were always 100 percent operational throughout the virus crisis. Our CommandNet, internet public servers, shared drive and file servers were never infected."

Connell explained in an e-mail message to employees that although SMDC's operating system was not infected, some workers who use Web services were indirectly affected because anyone who attempted to browse an infected Web site or whom was routed through a path that was clogged as a result of the virus would find services slow.

"Once a Web server is infected, it creates traffic inside a subnet, creating traffic in addition to what comes in from the outside," said Connell. "That increase in traffic clogs the bandwidth, slowing everything down—or in some instances forces a device or a server to shutdown."

Government officials acknowledge that public systems are under constant attack from hackers other than computer terrorists. Ten years ago, officials estimated that perhaps 500 computer viruses were virtually living in the Internet. Today, experts believe there may be

more than 60,000. According to one estimate, SMDC faces as many as 1,000 attacks every month. Officials at Redstone's Army Aviation and Missile Command (AMCOM) recently told the *Huntsville Times* that more than 1,200 attacks were made on their system following the Code Red outbreak.

Working smarter, not harder, takes on new meaning when dealing with faster, meaner, and smarter computer bugs. SMDC's constant vigil is aided by a Joint Task Force Computer Emergency Response Team that alerts government agencies to new threats.

"SMDC is no different from the commercial world when it comes to targets," said Aubrey Pinkerton, an SMDC network manager. "We are always going to be a target for hackers, so we are always alert to new threats. And we have measures in place, such as firewalls to capture things before they can take effect. The response team alerts us and we go into action to shut off paths from the outside until we apply 'patches' and other protections, such as notifying all our employees about a new threat. When everything is in place, we open up again."

Types of malicious computer code

Three basic flavors of malicious codes currently exist: the Worm, the Trojan Horse, and the Virus.

Codes that burrow into a computer's memory are called **Worms**. A variety of worm that hibernates for later activation is sometimes called a **Mole**. Worms and moles can lay dormant for long periods of time, then suddenly spring to life by activating, altering, or destroying files and using up a system's resources.

If you stayed awake during history class, you know a **Trojan Horse** isn't what it seems. Disguised as a sound file or other desirable item, a Trojan can alter system files and/or create a **back door**. A back door can allow access to unauthorized users. For that reason, Trojans are of great concern to government agencies and private corporations.

Viruses can also alter or corrupt system files. They generally attach and insert themselves into a computer file, then infect other programs to slow down a computer by taking up resources. Unchecked, a virus can shut down a computer's memory or hard drives.

Common names: Most computer ailments have names, such as Jerusalem, Tequila, Michelangelo, Melissa, Love Bug, Stages, SirCam, Code Red, and Peachy.

Computer help for home

Carnegie-Mellon University's non-profit Emergency Response Team Coordination Center posts warnings as computer viruses appear. They operate a Web site where anyone can get up-to-date information on viruses: www.cert.org. Microsoft also offers free information on their Web site, www.microsoft.com.

Commercial software offer online updates as new viruses emerge. McAfee VirusSan and Norton AntiVirus programs are available free for Federal employees through their local HelpDesk.

So you've got suspicious mail—What does the U.S. Postal Service say to do with it

In light of recent cases of anthrax exposure and contamination, at least some of which appear to have been delivered through the mail system, the following guidelines are provided from the United States Postal Service in question and answer format:

■ What constitutes a suspicious parcel? Some typical characteristics postal inspectors have detected over the years, which ought to trigger suspicion, include parcels that:

- Are unexpected or from someone unfamiliar to you.
- Are addressed to someone no longer with your organization or are otherwise outdated.
- Have no return address, or have one that can't be verified as legitimate.
- Are of unusual weight, given their size, or are lopsided or oddly shaped.
- Are marked with restrictive endorsements, such as "personal" or "confidential."
- Have protruding wires, strange odors or stains.
- Show a city or state in the postmark that does not match the return address, or has no return address.

■ What should I do if I receive a suspicious piece of mail?

- Do not handle the piece of mail.
- Notify your supervisor and immediately contact military police or local law enforcement.
- Make sure that damaged or suspicious packages are isolated and the immediate area cordoned off.
- Ensure that all persons who have touched the mail piece wash their hands thoroughly with soap and water.
- List all persons who have touched the letter and/or envelope. Include contact information. Provide the list to responding law enforcement.
- Place all items worn when in contact with the suspected mail piece in plastic bags and keep them wherever you change your clothes and have them available for law enforcement agents.
- As soon as practical, shower with soap and water.
- If prescribed medication by medical personnel, take it until otherwise instructed or it runs out.

Alabama quality awards touch SMDC

by **Becky Proaps**
Huntsville

The Ballistic Missile Targets Joint Project Office (BMTJPO) and the U. S. Army Space and Missile Defense Command's Space and Missile Defense Battle Lab have won big again. BMTJPO won the overall 2001 Alabama Quality Award in the Service Sector category. The Battle Lab Studies and Analysis Division placed at the bronze level; the Battle Lab Advanced Research Center placed at the silver level and the Battle Lab Operations Division placed at the silver level, all in the service category of the 2001 Alabama Quality Award Team Showcase.

BMTJPO prepared a 50-page submission in April 2001, explaining its organization and merits. It also hosted a two-day site visit in September in which the senior leaders gave briefings to the examiners, along with a visit to Lockheed to show some of the hardware BMTJPO is responsible for managing. According to a letter received from the award board, BMTJPO was chosen because the examiners and judges were impressed with the productivity and quality efforts BMTJPO, its staff members and others associated with them have been engaged in, their impacts, and the commitment and leadership shown in these efforts. The BMTJPO is the sole executing agent for the Ballistic Missile

Directed Energy symposium held in Huntsville

The Directed Energy Professional Society in cooperation with the Office of the Secretary of Defense, the U.S. Army Space and Missile Defense Command, the U.S. Air Force Research Lab, the U.S. Navy Sea Systems Command, and the U.S. Marine Corps sponsored the 4th Annual Directed Energy Symposium Oct. 29 through Nov. 1 in Huntsville, Ala.

The symposium brought together government, industry, and academic leaders for discussions of basic research and technology efforts, current programs, and the future of directed energy for national security purposes.

The symposium provided forums for the interchange of scientific and technical information in the fields of high energy lasers (HELs), high power microwaves (HPMs), and HEL active sensing.

Some of the unclassified sessions included short courses in Lasers and Laser Optics, Beam Control System Design, Introduction to Optical Propagation, High Power Laser Beam Control Progress, NAS Advanced Optics Technologies, HP Microwave Systems, and Fundamentals of Laser Lethality Analysis.

Symposium sessions included a look at the congressional, DoD, BMDO, service, Department of Energy (DoE), and industry perspectives of the directed energy vision.

Other public domain sessions explored DoE Laboratory Programs and directed energy technologies.

The Directed Energy Professional Society was founded in 1999 to foster research and development of directed energy technology for national defense and civil defense applications through professional communication and education.

Defense Organization Consolidated Targets Program for the Department of Defense.

The Battle Lab Advanced Research Center and the Task Sheet Database Team received their silver level Team Showcase awards for their systematic team approach to continuous improvement and use of quality management tools. The bronze level, awarded to the Battle Lab Studies and Analysis Campaign Plan Team, was also for their systematic team approach to continuous improvement.

The Alabama Quality Award is sponsored and administered by the Alabama Productivity Center on the University of Alabama campus in Tuscaloosa, Ala. The award recognizes and honors orga-

nizations that are using effective productivity and quality improvement strategies, techniques or practices that could be shared with other organizations with the expectation that they will contribute to the overall economic well-being of Alabama. The awards are presented annually to private sector companies and non-profit agencies demonstrating such commitment to productivity and quality.

The awards ceremony will be the culmination of a two-day conference to be held in Birmingham, Ala., Nov. 27 and 28 at the Richard Scrushy Conference Center.



Photo by Jonathan Pierce

(At left) Don Underwood, director of Vehicle Engineering at PEI Electronics discusses the hybrid Humvee with its demonstration package for the heat capacity solid state laser with Roy Priest, district representative for U.S. Congressman Bud Cramer.

Hybrid humvee sports laser demo

The idea of having highly mobile vehicles traversing the battlefield, shooting down short-range rockets and artillery and mortar rounds seems to be the stuff of science fiction. No longer.

The hybrid high mobility multi-wheeled vehicle (HHMMWV or Humvee) already exists, and the tactical weapons-level heat capacity solid state laser isn't far behind.

PEI Electronics, located next door to the SMDC facility in Huntsville, put the hybrid Humvee on display during the Directed Energy Symposium in early November.

According to Dr. Randy Buff, SMDC Technical Center Weapons Directorate, the command had spent several years trying to find a vehicle that could power a solid state laser weapons system without having to add a towed generator. Nothing seemed to fit the test of mobility and reduction of mass until they discovered the hybrid Humvee right next door at PEI Electronics.

The hybrid Humvee runs off diesel fuel and has high capacity batteries that can store a lot of energy, according to Don Underwood, director of Vehicle Engineering at PEI Electronics. In fact, it has so much battery power that the

vehicle can be driven under electrical power alone. In effect, the diesel engine is also the power source for the batteries. With a few modifications, it was determined the hybrid could be both the vehicle and the power source for the solid state laser weapon now being developed.

The hybrid, according to Underwood, has the capability to be twice as fast as normal Humvees, it can accelerate at least twice as fast, and has twice the fuel economy at more than 16 mpg.

The laser weapon, when developed, will likely have three 10-round magazines. A shot is a one-second burst of 200 pulses. Underwood said that when the magazine is depleted the hybrid Humvee will only need 20 minutes to recharge the "magazine," its own batteries. Effectively, the hybrid Humvee makes its own "bullets" from diesel fuel.

SMDC's High Energy Laser Systems Test Facility (HELSTF) located at White Sands Missile Range, N.M., recently received a 10-megawatt solid state laser from Lawrence Livermore Labs.

The goal at HELSTF and for the hybrid Humvee solid state laser is to develop a 100-megawatt heat capacity solid state laser.

Ward honored with Saint Barbara award

by Jonathan Pierce
Huntsville

The gods of thunder have looked with favor on one of SMDC's own. Kay R. Ward was honored Oct. 20 by being inducted into the Honorable Order of Saint Barbara at a ceremony conducted by the Redstone Arsenal/Huntsville Ala., Chapter of the Air Defense Artillery Association.

The award honors individuals who have demonstrated the highest standards of integrity and moral character and an outstanding degree of competence in serving the U.S. Army air defense artillery or field artillery with selflessness.

Saint Barbara is the patron saint of air defenders and field artillerymen alike. Legend has it that Saint Barbara was the beautiful daughter of a wealthy man named Dioscorus who lived in Asia Minor

around 300 A.D. While he was gone on a trip, Barbara heard and accepted the teachings of Christ. When her father returned, he was infuriated and beheaded her. He was struck and consumed by lightning. Barbara became known as the patron saint in times of danger from thunderstorms, fires, and sudden death. The advent of gunpowder and cannons, and their tendency to explode instead of fire, made her the welcome patron of artillerymen against accidental explosions.

Ward has just completed an assignment as the U.S. Army Space and Missile Defense Command's (SMDC) assistant deputy chief of staff for Strategic Planning and Analysis and is currently providing support for the SMDC chief of staff.

Ward has served the field artillery and air defense artillery branches in the Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System Project Office, the Unmanned Aerial Vehicles Joint Project Office, the Anti-Satellite Joint Program Office, and the Aerostat Joint Project Office. She has also served in the Program Executive Office (PEO) Fire Support, and in PEO Tactical Missiles. She entered program management in the Pershing Program Office.

Sensors Directorate picked for President's APIC run

Sensors Directorate of the U.S. Army Space and Missile Defense Technical Center has been selected by the Department of the Army to compete for the President's Quality Award. This is the first time that an organization from this command has been selected. This competition is based on the Army Performance Improvement Criteria (APIC), a Malcolm Baldrige-based criteria.

The Space and Missile Defense Technical Center took a novel approach in implementing the Army Performance Improvement Criteria (APIC). Rather than try to take on the entire organization, they chose to initiate a pilot project within the Sensors Directorate. Upon completion of the deployment of the criteria, and the analysis of results data this office will use an Integrated Process Team to accomplish full deployment within the center. The goal is to institutionalize this management tool within the entire Technical Center.

The Sensors Directorate won third place in this year's SMDC Commander's Award Competition. After receiving the feedback report from the command, the directorate reworked their package and forwarded it to the Department of the Army Competition where it was judged along with 12 other packages. The Department of the Army forwarded six assessment packages to the Office of Personnel Management for competition in the President's Quality Award. The results of that competition will not be known until Summer 2002.



Kay Ward (center), a new recipient of the Order of St. Barbara, is joined by former recipients, Ms. Nancy E. Archuleta (left), CEO of Mevatec, and Ms. Maxine Maples-Kilgore, director, Southern Region Army Acquisition Corps. The St. Barbara award honors individuals who have made significant, continuing contributions to the field artillery and air defense artillery branches of the U.S. Army.

SMDC Organization Overview

Army TENCAP – Real support to the real warfighter

As the Army transforms itself into the Objective Force, the need for timely and accurate combat information will increase in importance. Dispersed, highly mobile forces, who are equipped with the latest suite of weapons, will require an information system that is flexible, robust, and reliable. Information provided by Intelligence, Surveillance, and Reconnaissance (ISR) sensors that are hosted on a variety of platforms will be passed quickly to the commanders who engage with the enemy throughout the length of the battlefields of tomorrow.

Regardless of the source of data, Army Tactical Exploitation of National Capabilities (TENCAP) systems will play a vital role in any future U.S. conflict. Sensors will include not only the Signals Intelligence (SIGINT) and Imagery Intelligence (IMINT) systems with which we are familiar, but also will include the category of sensors we refer to as Measurement and Signature Intelligence (MASINT), using special processing and data combining techniques to provide intelligence information. The U.S. Army Space and Missile Defense Command's Army Space Program Office (ASPO) is providing leading-edge, tactical ground stations that bring this critically needed data to the warfighters at the forefront of any conflict.

In 1973, the Army established the ASPO to perform the mission of executing the Army TENCAP program, serving as the unique technical and fiscal interface with the national program offices and managing the

TENCAP materiel acquisition process. The Army's TENCAP program is based on exploiting the current and future tactical potential of national capabilities and integrating these capabilities, as rapidly as possible, into the Army's tactical decision-making process.

National systems are designed to support strategic requirements. The ASPO leverages national technology to provide information from these strategic systems to tactical levels. This data provides an accurate and current picture of both the enemy and the terrain during planning and execution stages. In Haiti, TENCAP systems provided the primary source of imagery directly to the Joint Task Force (JTF) commander's analysts, enabling them to plan the operation and execute the initial assault. Another relevant example occurred during OPERATION DESERT STORM where TENCAP systems provided the majority of targeting support for deep operations and imagery for support of operation planning/maneuvering for both the XVIII Airborne and VII Corps.

TENCAP systems are also a significant source of quick-reaction capability support to humanitarian efforts. After Hurricane Andrew, TENCAP systems provided rapid and detailed damage assessment to the task force commander responsible for providing support to the relief effort. TENCAP secondary dissemination and intelligence broadcast capabilities also foster continuing awareness through all phases of operations, enabling the tactical commander to see, hear, and

target deep in today's battlefield, and then to assess the effects of shooting deep.

The ASPO has developed and fielded more than 60 systems to both Army and Air Force tactical units. After 20 years of service, the ASPO charter was revalidated in 1993. Today, the Army TENCAP program is the largest and most visible of the individual service's TENCAP programs. The most recent system in the TENCAP inventory is the Tactical Exploitation System (TES), currently being fielded across the Army force structure. It is replacing earlier systems, now designated as legacy systems, at echelons above corps, and in corps and division echelons.

The TENCAP program embraces all phases of materiel development, system acquisition, and sustainment. ASPO provides cradle-to-grave logistical support through a combined effort of government and contractor personnel and facilities. Key factors for success include an environment emphasizing stable funding and low-density acquisition, maximum use of commercial technology, minimal use of military specifications, and managed competition. By tailoring existing technology, leveraging the best commercial practices, and using commercial-off-the-shelf and government-off-the-shelf software, ASPO minimizes risk while maximizing efficiency. Strong user involvement and a robust operations and maintenance program in a vigorous pre-planned product improvement environment help ensure programmatic success.

Fielding begins for Grenadier BRAT

The Grenadier BRAT system is a blue-force tracking tool being fielded by the Space and Missile Defense Command (SMDC) Army Space Program Office (ASPO). Beyond line-of-sight Reporting and Tracking (BRAT) gives commanders the ability to track friendly forces in near-real time deep on the battlefield—even if line-of-sight communications with those forces are not possible.

The primary components of the Grenadier BRAT (GB) system include the transponder, a hand-held terminal (HHT), a small (approximately 3.5") UHF transmit antenna, and a Global Positioning System (GPS) receive antenna. A GB Planning Computer is also used to create, manage, and load the GB system files prior to a mission. The transponder measures 6" x 6" x 3" and weighs about 5 lbs, which makes it small and light enough to be used in a variety of configurations. GB can be either man-packed or mounted on military vehicles or aircraft. The man-packed option allows even dismounted patrols the ability to report their location information to higher echelons. In the man-packed configuration the GB system uses a rechargeable battery pack, but when used in vehicles or aircraft the GB can operate from vehicle or aircraft power.

GB's Hand-Held Terminal allows users to interactively control the GB system during a mission. Through the HHT, users can turn the GB system on or off, control how often the GB system transmits location information, and include short messages (called "brevity codes") within the GB transmission. For example, a helicopter might transmit a brevity code meaning "enroute" while moving to an objective, and an "arrival" code upon reaching that objective. The helicopter crew could also use the HHT to configure the GB transponder to transmit only once every five minutes before crossing the Forward Line of Troops (FLOT), and then increase the frequency of transmission to every 15 seconds as they fly over enemy territory giving the commander more frequent movement updates.

Grenadier BRAT calculates position information through the signal it receives from GPS satellites. GB transmits this data along with unit identification and a brevity code via a special waveform. This waveform addresses a concern that many soldiers have with blue-force tracking systems—that an enemy could potentially intercept the tracking signal for surveillance or targeting purposes. The waveform has very low probability of intercept, a low probability of detection, and is encrypted. It is generally indistinguishable from radio background noise, so it provides the user with excellent security

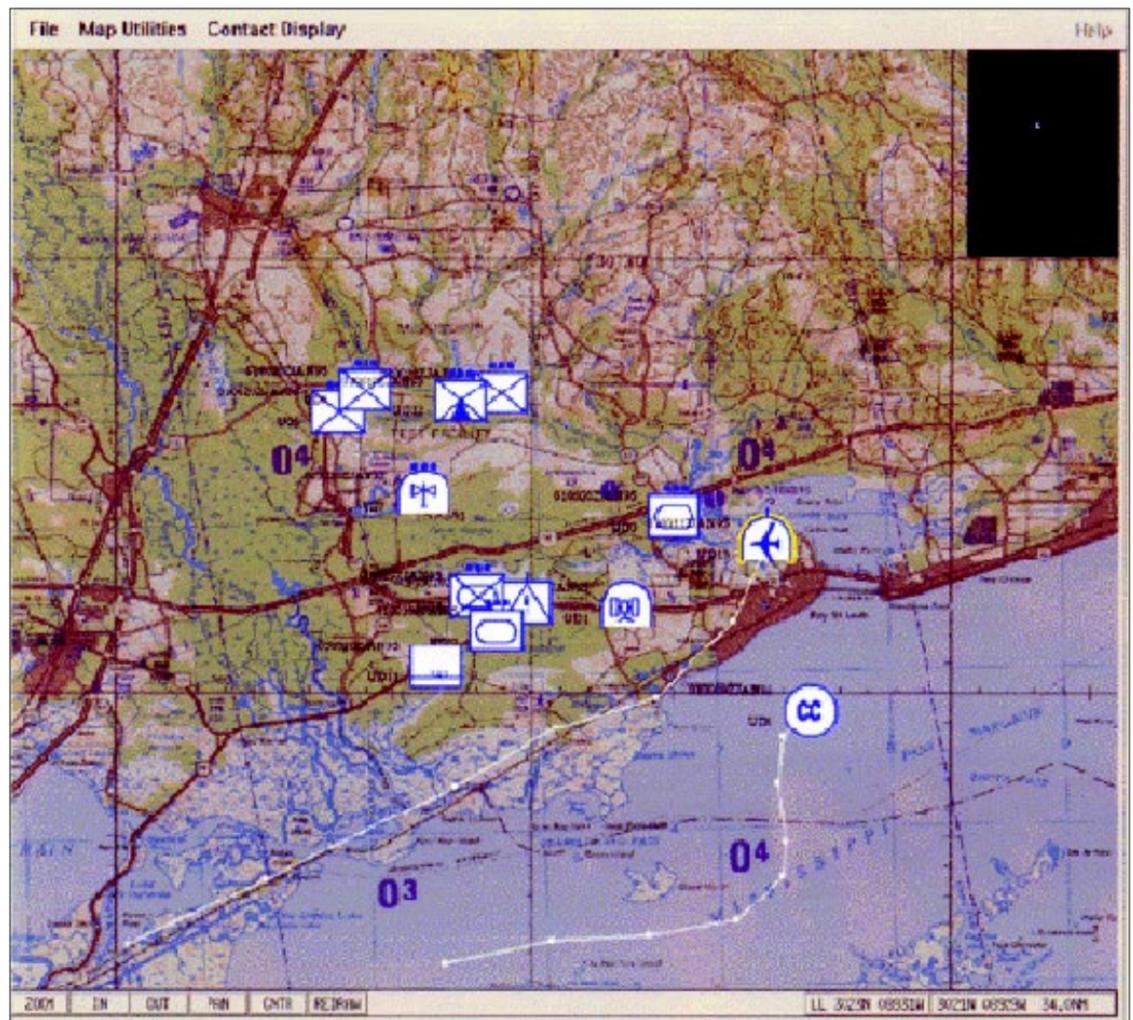
and minimum risk of exposure. The GB transmission also uses a very short burst that is spread over several frequencies (spread spectrum transmission).

Grenadier BRAT uses existing collection and dissemination architectures to provide its data to the commander. Blue-force tracking data can be received and processed with Army Tactical Exploitation of National Capabilities equipment and displayed as standard military symbols. When broadcast over the Integrated Broadcast System (IBS), any unit with a Tactical Receive Equipment (TRE) capability can receive GB information, to include units with the Common Ground Station (CGS) and special operations forces with the SOF Intelligence vehicle (SOFIV). GB data can be displayed as part of a unit's Common Operational Picture (COP) on a variety of platforms, including the Global Command and Control System—Army (GCCS-A), the Maneuver Control System (MCS), and the All Source Analysis System—Remote Workstation (ASAS-

RWS). GB's blue-force data can be combined with red-force data to provide the commander with a near-real time view of both friendly and enemy forces on the battlefield.

GB prototypes have been in used in several exercises since 1995, including U.S. Army South force protection exercises; exercise FOAL EAGLE in Korea, ROVING SANDS in New Mexico, and 18th Aviation Brigade's TIGER RAGE. GB prototypes continue to be used in real-world operations today, including Operations NORTHERN WATCH and SOUTHERN WATCH in Iraq.

Fielding of Grenadier BRAT began in October with the 5th Special Forces Group in Kuwait, followed by units in Bosnia, Kosovo, Germany and Italy. I Corps, XVIII Airborne Corps, U.S. Army South, and the 25th Infantry Division will follow shortly afterward. Their experience with the initial Grenadier BRAT fielding will enhance an eventual Army-wide Grenadier BRAT device. For more information on the Grenadier BRAT system, contact Maj. Charles A. Wells at Charles.Wells@aspo.army.mil.



Grenadier BRAT blue force data displayed on an Army TENCAP system.

First RDAP members graduate

The first group of acquisition workforce members graduated from the Southern Region's Rotational Developmental Assignment Program (RDAP) Oct. 23. The graduates, all from the Huntsville area included: Deana Braden, Rhonda Brock, Kari Elliott, Arthur Seaman, James Springer and Devin Whitaker. Participating organizations included: PEO Aviation, PEO Tactical Missiles, PEO Air and Missile Defense, and the Acquisition Center.

Brigadier General (P) John Urias, deputy commanding general for Research, Development, and Acquisition, U.S. Army Space and Missile Defense Command, served as the keynote speaker. He recognized and thanked graduates and supervisors for their support of this pilot program.

The RDAP will begin its second year in January 2002 and is being expanded to the Northeast and National Capital Regions.

The RDAP is open to acquisition

workforce members who are Level III certified in their primary acquisition career field or who meet their position certification requirements. Selectees are placed in developmental positions throughout the local acquisition community based on the needs of the organization, the Army Acquisition Corps (AAC), and the individual. The length of the assignment is typically one year, but they can vary from six to 24 months.

The RDAP was developed by the Southern Region to support the AAC objective of having a highly skilled and multi-functional workforce with strong management and leadership skills. The objectives are to broaden and enhance Acquisition and Technology Workforce members' management and leadership skills and competencies; develop multi-functional acquisition skills and competencies; and to provide opportunities for increased levels of responsibility and skill enhancement through on-the-job training.



Arthur Seaman (left) listens to Randy Richardson, his supervisor in the RDAP program, as they go over a report.

Army Guard Space battalion activated

Colorado ARNG 193rd Space Support Battalion

COLORADO SPRINGS, Colo.—Two firsts took place on the grounds of Peterson Air Force Base Sept. 28 as the Colorado Army National Guard's 193rd Space Battalion was activated and became the third battalion in U.S. Army Space Command family.

The event heralded a first for the Army National Guard, as a Colorado Army unit becomes the first in the nation with a Space mission. The creation of this new battalion is part of a Total Army effort with Army Space Command, which began back on Jan. 20 with the establishment of the 193rd, and weekend training with Army Space Command personnel.



U.S. Army photo by Sharon L. Hartman

(Left to right) Colorado Army National Guard Commander, Brig. Gen. Ronald G. Crowder holds the colors for the COANG 193rd Space Battalion with the battalion's commander Lt. Col. Michael L. Yowell and Sgt. Joseph Allen, Jr., an Army Space Support Team topographer, looking on as Command Sgt. Maj. Daniel Marques of the COARNG 89th Troop Command unfurls the flag signifying the activation of the battalion.

Soldiers, civilians and VIPs joined Brig. Gen. Ronald G. Crowder, commander of the Colorado Army National Guard, as he officially activated the battalion during the uncasing of the 193rd colors with the assistance of Command Sgt. Maj. Daniel Marques from the 89th Troop Command.

"We feel like we have a great symbiotic relationship in the Colorado Guard, U. S. Army Space Command and U.S. Army Space and Missile Defense Command, and I know it is through the initiative that Brig. Gen. Richard Geraci brings to this," he said after the ceremony.

The battalion, which currently has 30 soldiers, is commanded by Lt. Col. Michael Yowell.

Training for the new battalion is centered on two six-member Army Space Support Teams (ARSST) and a three-member information operations and mobile technology team.

The guard's two Space Support Teams will supplement Army Space Command's ARSSTs. These teams, which are deployed to various Army Corps elements, will provide key Space capabilities and products directly to the warfighter in the field. They include satellite advance notice, global positioning, Space weather, imagery, intelligence support, and satellite communications.

The Colorado Army National Guard Space Support units should be operational by fall of 2002. According to Army Space Command officials, Space has and continues to play a key role in the ongoing Army transformation, and the Colorado Army National Guard is one of the key players.

The battalion's mission is to train their teams and sections according to the standards set by the commander of U.S. Army Space Forces. In addition they will have a unique reporting structure normally not seen in most Guard units.

In peacetime, they will receive support through state Army National Guard channels with the chain of command proceeding through the 89th Troop Command to the Ground Force commander in Denver. If called upon during a national emergency, the 193rd will fall under the direct control of Army Space Command.

Members of the new battalion are currently based out of Army Space Command headquarters pending funds for acquisition of a permanent building in Colorado Springs.

Colorado National Guard trains with ARSPACE

COLORADO SPRINGS, Colo.—"Hey, this is real-world training," observed Sgt. Donald Purvis with the Army Space Support Company, 1st Space Battalion, U.S. Army Space Command. He was speaking to members from the Colorado Army National Guard's 193rd Space Battalion during an October weekend training session at Army Space Command facilities in Colorado Springs, Colo.

Purvis, one of several Army Space Command soldiers serving as facilitators, wanted the Guard personnel to know the urgency of their training on Army Space Support Team skills.

Less than one month after the historic activation of the 193rd, two of its Space support teams faced the challenge of hands-on training after months of instruction.

The approach was simple: On Saturday each team first disassembled Space support equipment set-up for operation. They then packed it up and prepared it to ship out as if it were actually being deployed. Afterwards the soldiers unpacked all equipment.

On Sunday morning, both teams unpacked equipment from the previous day and configured two complete Space support set-ups for a morning exercise.

"I'm new in the unit," said Staff Sgt. Shelly Biller, an Army Space Support team leader non-commissioned officer in charge for team #10 (a new team being formed in the battalion.)

Biller, from Elizabeth, Colo., is a network security manager for the Colorado Army National Guard. "We have a lot of personalities and background to help us out, as well as the experience of bringing it all together. It is going to be great."

The most important lessons learned during this past weekend's training has been, according to Biller, "Knowing what systems there are, what they are used for, and how they help our troops out in the field."

An Army Space Support Team provides valuable space capabilities and products to the warfighter in areas such as satellite communications, global positioning system navigation, theater ballistic missile warning, satellite imagery and even Space weather which can affect communications and satellite links.

As the exercise progressed throughout the morning and into the afternoon, planned glitches—and some not planned—occurred causing comments to abound from Guard participants.

Despite troubles with equipment and planned hurdles such as communications links and satellites going offline, the teams showed resiliency.



Photo by DJ Montoya

(Standing) Sgt. Donald Purvis with the Army Space Support Company, 1st Space Battalion, ARSPACE, assists Staff Sgt. Brian Harper (left) and Staff Sgt. Matthew Pollock (right), both from the Colorado Army National Guard's 193rd Space Battalion.

"This weekend is basically a collection of everything we've learned since January," said Sgt. 1st Class Joseph Thill, Army Space Support team leader for team # 9.

Thill currently works full time for the Colorado Army National Guard Counter Drug Program.

Assessing the training for the weekend Thill said, "We started in January with the basics of this is what an Army Space Support Team does.

"Now it is taking all that conceptual knowledge we've learned over the last 10 months and putting it all together into [the] 16 hours of this exercise," Thill said. He said the training would display "what things we have a good lock on," and "what it is we still need to work on."

"Only 18 more training days until EXERCISE ULCHI-FOCUS LENS in Korea," said Maj. Ralph H. Trenary, Army Space Support Team chief of the 193rd, encouraging the soldiers toward their goal.

"I'm confident we will be ready to participate in next year's war game exercise in Korea," he said.

Identity Theft : It

by Dan Coberly
Huntsville

Usually, there is only one you.

But, when a collection agency calls demanding you pay past-due accounts for things you never ordered or, the supermarket refuses your check and you normally pay bills on time—someone may be impersonating you. If someone steals your identity, you could find yourself fighting a long, frustrating battle to clear your good name.

Since July 1, 2001, major credit bureaus in the United States were allowed to release your credit information, mailing addresses, phone numbers and other personal information to anyone who requests it. But you can “opt out” of that situation by dialing 888-567-8688. Generally, victims of credit and banking fraud are liable for no more than the first \$50 of the loss (15 USC 1643). However, the victim must notify financial institutions within two days of learning of the loss, although that is often waived. The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified in part at 18 U.S.C 1028) is the federal law directed at identity theft.

In most cases, a conviction for identity theft carries a maximum penalty of 15 years imprisonment, a fine and forfeiture of any personal property used or intended to be used to commit the crime. Other laws on the books involving wire fraud, mail fraud, social security, etc., are felonies carrying penalties as high as 30 years in prison, fines, and criminal forfeiture. Small consolation to the victims when their reputation and finances are damaged.

The Fair Credit Reporting Act establishes procedures for correcting mistakes on your credit record. The Truth in Lending Act limits liabilities. Victims usually are not saddled with paying their imposter's bills, but they are often left with a bad credit report and must spend months or years regaining their financial health. It often costs victims time and money to correct. The Fair Debt Collection

Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection. Victims find there is almost no help from authorities as they attempt to untangle the web of deception another person used to impersonate them. Fraud departments at financial institutions are usually a victim's best friend because they too, have a vested interest in solving the problem.

Nationally, 500,000 to 700,000 cases pop up each year, costing victims more than \$765 million. According to the U.S. Treasury's Financial Crimes Enforcement Network (FCEN), the number of identity thefts directly reported by banks and other financial institutions more than doubled last year. In just four months, from January to the end of April 2001, the FCEN received 332 reports of bank-related identity theft compared with 637 cases during 2000 and 267 cases in 1999. In 1997, the first year national bank records were kept, only 44 bank cases were reported. Among ordinary citizens, Washington, D.C., is tops when it comes to identity theft. Annually, 20 incidents occur for every 100,000 people in the Washington, DC, area. Statistics for Huntsville were not available, but a local law enforcement official acknowledged a “growing problem.”

Gangs of thieves buy and sell stolen identities like commodities, according to government reports. Often, they begin by obtaining a credit card number or bank statement. But the basic bandit's best tools are simply your social security number and date of birth. A home address and telephone number are icing on the cake.

Armed with that information, an identity thief can begin impersonations by obtaining credit cards and opening bank accounts. Thieves can use your identity to sign up for cell phones, get a driver's license, or buy a car. And when you live in Alabama, and someone in Florida cashes a bad check in your name, it can be difficult to determine who has jurisdiction over the crime. That's one of many reasons why it seems so relatively easy for identity theft to occur, making it one of the fastest

growing crimes in our nation.

Jonathan Kirby, security manager at the Redstone Federal Credit Union, advises members to shred any personal or financial information leaving their home.

“People simply throw too much information away,” he said. “When they do, that makes it easy for anyone to retrieve personal information from the trash. We advise our members to check their statements very carefully, and to contact us immediately if there is a discrepancy.”

Kirby said some people think identity fraud is only about stolen credit cards or someone getting credit in their name. He said people don't think about their checking or savings accounts.

“Our employees are trained to pick up on certain things that may indicate someone is attempting to assume a member's identity. For example, an employee may get a call asking for information about an account and something just doesn't seem right about the call. Or, we notice unusual activity on the account and we contact the member and monitor it. We have thwarted several fraud attempts here before they were successful,” Kirby said.

“People simply throw too much information away,” he said. “When they do, that makes it easy for anyone to retrieve personal information from the trash.”

Sue Ellen Sandoval, handles fraud cases for the Associated Credit Union in Atlanta, where many federal employees bank. She said many people use their mother's maiden name as a code but don't always protect that name. “People really do need to be careful with any kind of personal information, including their mother's maiden name,” she advised.

Kirby and Sandoval agreed that mail can also be stolen from your mailbox or trash. For example, you pay a bill and leave it in your mailbox. Most people work and aren't at home watching the mail. Anyone who drives by can see the red flag, and they could end up with your signed check and your account number.

“If you're going to mail bill payments, it's always a good idea to use a government mailbox. And you can't go wrong shredding any pre-approved credit card applications you don't want rather than just tossing them in the trash,” Sandoval said. “People should also be careful when using a computer to conduct financial transactions, to ensure that it is a secure site. Look for an ‘S’ after the ‘http’ on the address line,” she suggested. “And never give out any personal or financial information on the phone unless you initiated the call.”

Internet Crime

Law enforcement officials will tell you to think beyond credit cards when it comes to information about your identity. They too, remind people to shred or burn any kind of personal information. Computer geeks will tell you that the same dangers exist if you sell, throw away or donate your old computer without properly deleting personal files.



Could happen to you

Last year, the Treasury Department added "computer intrusion" as a category of suspicious activity for banks to monitor and report. The term is defined as "gaining access to banks' computer systems to steal funds or data, or to try to damage the systems." During the first year of the reporting requirement, the Treasury received 83 substantiated reports of computer intrusions, with 60 percent of the cases involving the banks' own employees trying to embezzle funds or perpetuate other frauds.

Because most of us take our personal identity for granted, criminals have also organized to hack financial computer systems, infiltrate banks, and steal mail. One recent scheme included hacking and attempted extortion of at least four banks by a Russian programmer earlier this year. Other recent innovations include creation of phony bank websites to steal customer data. A recent increase in terrorist activities involving false or stolen identities makes combating the crime more urgent, prompting some citizens and politicians to call for a national identity card.

If Internet commerce is to succeed, government sources have said electronic stores must be built upon consumer confidence. Fraud is the biggest threat to consumer confidence. That's why three agencies, the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), and the Internet Fraud Complaint Center (IFCC)—a joint effort by the FBI and National White Collar Crime Center—have taken the lead in combating Internet fraud.

Although government oversight of 21st century scams is still evolving, the FTC sits at the helm of the cyber-patrol effort. The FTC's Bureau of Consumer Protection now serves as the civil sentry of the Web. Their experts have identified and nabbed a new breed of hacker called "pagejackers" as far away as Australia and Portugal. Pagejackers change a tiny piece of code on a Web site so that visitors are automatically redirected to other sites.

Once redirected, it's easier for them to

steal personal information. Recently, the SEC's Internet enforcers tracked down a perpetrator of yet another electronic scam, called "pump and dump." Someone using a false identity spreads false information about a publicly traded company in order to reduce or inflate stock values. Often, sending spam emails to stolen email addresses spreads the disinformation.

In the first six months of one operation, from May to November 2000, the IFCC, received more than 20,000 complaints and referred more than 6,000 of them to regulatory and law enforcement agencies around the world.

DoD identifications

Passports, military and civilian ID cards, even Department of Defense stickers, parking permits, and government license plates are also subject to use for identity theft, prompting recent government warnings. DoD personnel were reminded to remove the identifications when ownership changes and to report any thefts or attempted thefts, and anyone who wants you to leave your decal or other identification on the vehicle. According to media reports, several incidents involving DoD decals took place at the Pentagon and in the Washington and Baltimore areas throughout September.

Minimize your risk

Experts say the best way to protect yourself is to be informed and to be proactive. SMDC employees will find the Intelligence and Security Division wants to help. Visit the staff website under "Intelligence and Security" at http://commandnet/I&S/Intell_Security.html. There, you will find ingenious ways identity thieves can steal your identity, your codes, and your money. You will also find dozens of countermeasures you can take to keep your family and yourself safe.

Take action!

Sign your credit cards as soon as they arrive. Write "Check ID" next to your signature. Carry only one or two cards with you. Keep the others at home in a safe place with a photocopy of the cards.

Keep a record of all credit card numbers, expiration dates, company addresses, and phone numbers in a secure location. Keep an eye on your credit card during transactions, get it back from the clerk as soon as possible. It is possible to "skim" electronic information from your card. Save receipts and compare statements. Once verified, shred receipts that contain card numbers.

The Social Security Administration has dropped the first five digits from the new, annual Social Security statement mailings to help protect your identity in case statements are lost or stolen. To learn more about the statement, visit www.ssa.gov/mystatement/.

Check your credit report frequently for inaccuracies of any kind. Reviewing your report will tell you if someone has applied for credit in your name, and if any accounts are being used without your knowledge. You can often obtain a free copy of your report online—but so can others. Sign up for a credit



©ArtToday, Used by Permission

monitoring service so you will know who is studying your finances.

What to do when you are a victim

Sandoval advises victims to contact financial institutions, local police and sheriff's departments, the social security office, and credit bureaus. She suggests placing "fraud alerts" on your credit file, to protect your name and social security number. The alert means that you have filed a "victim's statement"; any company that checks your credit then knows your information has been stolen and is required to contact you by phone prior to authorizing any new credit.

Be sure and ask how long the alert will stay on your accounts, and how you can extend it, if necessary. Keep a log of all conversations with officials and expenses incurred. Confirm conversations in writing and keep copies of all documents.

Credit bureaus

Bureaus advise that you immediately call all three major credit-reporting agencies. If there is a local office in town, call and arrange to visit in person to pick up a free copy of your credit report. Review it while there. File disputes on fraudulent information, stressing any fraudulent use of your accounts, or any not opened by you. Attach a copy of the police report to your file.

These measures may not entirely stop new fraudulent accounts from being opened by imposters. Ask the credit bureaus, in writing, to provide you with free copies every few months so you can monitor your credit reports. Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. You may also ask the bureaus to notify those who have received your credit report in the last six months to alert them to disputed and erroneous information.



©ArtToday, Used by Permission

Identity Theft: What to do if you're a victim

Remember, you are entitled to a free credit report if you are a victim of identity theft, if you have been denied credit in the past 60 days, if you receive welfare benefits, or if you are unemployed.

You can also contact your state's attorney general, the Federal Trade Commission, the Social Security Administration, and other agencies to correct the record:

Experian (Formerly TRW) 1-888-397-3742 or write P.O. Box 1017, Allen, TX, 75013. To opt out of pre-approved credit offers: 800-353-0809 or 888-5OPTOUT. Web: www.experian.com.

TransUnion: 1-800-680-7289 or write P.O. Box 97328, Jackson, MS, 39238. To opt out of pre-approved offers of credit 800-680-7293 or 888-5OPTOUT. Web: www.tuc.com.

Equifax: 1-800-535-6285 or write P.O. Box 740250 Atlanta, GA, 30374-0250. To opt out of pre-approved credit offers: (888) 567-8688. Web: www.equifax.com.

FTC Complaint Center

Identity Theft Hotline: 1-877-IDTHEFT (438-4338).

Call (202) FTC-HELP or contact www.ftc.gov/ftc/complaint.htm and fill out an on-line Complaint Form, or write the Consumer Response Center, Federal Trade Commission, CRC-240, Washington, DC, 20580. The FTC advises that if a bank seems to be ignoring you, send them a copy of the police report or other proof that you have taken legal action relating to fraud.

Social Security Administration

To contact the Social Security Administration, check your local phone book or call the **Fraud line:** 1-800-269-0271. To order a **Earnings and Benefits Statement:** 800-772-1213. Web: www.ssa.gov

Meanwhile, report anything suspicious to your credit card companies and law enforcement immediately. Keep credit card toll free reporting numbers handy so you can cancel your cards quickly. Quick reporting also helps protect you against having to pay unauthorized charges and should limit your liability. Early reporting also helps you to begin repairing the damage.

Contact all government, banking, and credit card agencies with whom you do business. Make sure you to file a written police report, obtain a copy, and note the complaint number.

Secret Service

The Secret Service has jurisdiction over financial fraud, but is usually does not investigate individual cases unless the dollar amount is high or you are



©ArtToday, Used by Permission

one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies or banks, as well as the police investigator, to notify the particular agent they work with. (web: www.treas.gov/usss)

U.S Postal Service

The U.S. Postal Inspection Service (USPIS) is another federal law enforcement agency that does investigate cases of identity theft. USPIS is the law enforcement arm of the U.S. Postal Service and has jurisdiction on all matters infringing on the integrity of the U.S. mail. You can locate the USPIS office nearest you by calling your local post office or checking www.usps.gov/websites/depart/inspect.

State and local governments

Many states and local governments have passed laws related to identity theft. Others may be considering such legislation. Where specific identity theft laws do not exist, the practices may be prohibited under other laws. Contact your state attorney general's office or local consumer protection agency to find out whether your state has any such laws. For a list of state offices visit: www.naag.org; to check the law visit www.consumer.gov/idtheft.

Direct mail and telephone calls

To remove your name from most mailing lists and to stop them from rent-

ing or selling your name to other companies, contact the Direct Mail Marketing Association, **Mail Preference Service**, P.O. Box 9008, Farmingdale, NY 11735 or **Preference Service Manager**, Direct Marketing Association, 1120 Avenue of the Americas, New York, NY, 10036-6700. Fax: (212) 790-1427. To avoid unwanted telemarketers, contact **DMA Telephone Preference Service**, P.O. Box 9014, Farmingdale, NY, 11735 or the Preference Service Manager listed above. In most cases, they will ask for your name, address and telephone number.

Fraudulent use of checks

First, contact the company the merchant uses. If possible, pick up new checks at the bank rather than have them mailed to you. When someone has stolen or forged your checks, contact:

CheckRite 800-766-2748
ChexSystems 800-428-9623 (for closed accounts)
CrossCheck 800-552-1900
Equifax 800-437-5120
National Processing Co. 800-526-5380
TeleCheck 800-710-9898

Privacy Rights Clearing House

For more information write:
1717 Kettner Ave Suite 105
San Diego, CA 92101

Ph: 619-298-3396

Web: www.privacyrights.org or pre@privacyrights.org

Radar tracks foreign space launches

by Preston Lockridge
Kwajalein Atoll

It's hard to hide from a 470-ton, 150-foot dish radar named ALTAIR (ARPA Long Range Tracking and Instrumentation Radar) or its smaller companion TRADEX (Target Resolution and Discrimination Experiment) co-located in the mid-Pacific Ocean. On Sept. 14, within 15 minutes after alarm, the U.S. Army Kwajalein Atoll Reagan Test Site's (RTS) ALTAIR radar's Space Surveillance Operations director, John Sullivan, is on-station with his crew and has initiated a wide scan to locate a New Foreign Launch (NFL) of a Russian Progress rocket. ALTAIR acquired the rocket and began tracking 27 minutes after launch with the rocket's payload achieving near-earth orbit. TRADEX acquired the launch complex as well to complete a pre-operational checkout.

ALTAIR is an Army-run Space asset which has primary responsibility for NFLs with TRADEX providing backup during times when ALTAIR is down for maintenance or up-grade. Either radar has a mini-

mum of three people on each crew to respond to NFLs, and is ready 24-hours a day, 7-days a week to track new launches in its role as a contributing sensor to the U.S. Space Command's Space Surveillance Network (SSN). Combined, the radars have provided data on more than 80 percent of every NFL activity that has taken place in Space this year.

According to Space Surveillance Department leader, Dave Greene, "ALTAIR's radar coverage typically begins 26 minutes 'time after launch' for Russian launches and 17-18 minutes for launches from China and other Asian countries. Once the NFL is detected, it is tracked to collect data that will assist the Space Command in identifying and cataloging the newly launched satellite." Without ALTAIR's coverage in the initial orbit, the Space Network would spend many hours searching for newly launched payloads.

The mission is to collect data and transmit that data to the Space Control Center and to other network sensors. "ALTAIR or TRADEX are typically the first radar in the U.S. Space Surveillance Network with coverage, due to our geographic location, which is positioned in the primary launch corridors of most non-cooperative foreign launches. They typically launch west to east in our direction to achieve Earth orbit," said Herb Schmidt, Operations Section leader.

The ALTAIR and TRADEX pairing also has a 100 percent success rate for the past three years in locating and tracking NFLs. Recognizing the significance of this achievement, USAKA commander, Col. Curtis Wrenn, Jr., said, "The ability to acquire and track NFLs is critical to our national interest. The hard work put into this task demonstrates the great teamwork and dedication throughout the organization."

These radars are highly sophisticated sensors used for deep Space, near-earth, and

orbital tracking. As one of the sensors in the Space Surveillance Network, ALTAIR detects, tracks, identifies, and catalogs all man-made objects in space. There are about 9,000 objects, 10 centimeters or bigger, that have been cataloged. Unfortunately there's an estimated 100,000 smaller objects that are not cataloged or tracked. TRADEX has the capability to track many of these smaller objects due to its high operating frequency. Efforts are underway to expand the use of TRADEX in tracking these objects. RTS uses these two sensors to track the 9,000 satellites/Space objects each year for the U.S. Space Command. The system performs more than 40,000 satellite-Space-object tracks each year for the command.

The ALTAIR and TRADEX radars also play an important role in acquiring and tracking rockets launched from various locations in the Pacific in support of national and theater missile defense programs. Most tests require the full spectrum of RTS sensors, which include other sophisticated radars and optical systems located on Roi-Namur and Kwajalein Atolls.

Two other range radars, Millimeter Wave and ALCOR radars, support the U.S. Space Command requirements for Space object identification, by providing high-resolution imagery of many near-earth orbiting objects.

The Reagan Test Site, organized as part of the U.S. Army Space and Missile Defense Command, is the nation's premier site for theater and national defense program missile testing and evaluation, a reputation it's earned for several reasons.

First, its isolation provides a safe impact area and vital operational security. The range also offers a combination of sophisticated, often one-of-a-kind radar and optical sensors, supported and operated by an outstanding mix of scientists, engineers, and technicians from various military and civilian backgrounds.

With the proliferation of tactical missiles around the world and with the increase in the number of rockets launching satellites into orbit, detection of new foreign launches at an early stage is critical to the security of the United States . . . so ALTAIR and TRADEX radars do not sleep. They remain on 15-minute recall status, 24 hours a day, 365 days a year as contributing sensors to the U.S. Space Surveillance Network.



U.S. Army Photo

The ALTAIR Radar points toward the heavens as it preforms its daily role of tracking foreign Space launches.



U.S. Army Photo

Space track operators track a new foreign launch at ALTAIR in support of the Space Surveillance Network and the U.S. Space Command.

SMDC tops in Army safety

The Space and Missile Defense Command received the Chief of Staff, U.S. Army Major Command Safety Award for achievements in accident prevention, systems safety, and risk management. Lt. Gen. Joseph Cosumano presented Max Tomlin, director of the Safety Office, with the award in a ceremony on Oct. 18.

Several factors lead to SMDC earning the award. SMDC experienced a 20 percent decrease for lost-time injuries and the lost-time injury rate from FY99. The commanding general also established and chaired a Command Safety and Occupational Health Council. In addition, the Safety Office became a member the Labor Management Partnership Council and the Command Inspection Program. CPR and first aid training was incorporated into the safety program.

Customers awarded the safety staff eight awards for their support during 2000. HQDA selected an SMDC safety engineer to chair the Army Insensitive Munitions Board and the International Systems Safety Society selected another as the Engineer of the Year for 2000.

To soar like the eagles. . .

by Dan Coberly
Huntsville

When Julie Hanson and her husband Toney want to get away from it all, they know exactly where to go. They go up, UP, and Away.... in their beautiful balloon, *Sun Dog*.

Julie is the crew chief for the hot air balloon piloted by her husband. They call their rides in the sky an "uplifting experience" because flying in a balloon is unlike anything you've ever done before.

A balloon may seem like primitive technology for someone like Julie, who works on the U.S. Army Space and Missile Defense Command's Research, Development, and Acquisition (RDA) staff. She calls ballooning "a slow, relaxing experience." Toney, a retired Navy master chief now working for a local defense contractor, calls it "a wonderfully positive way to adjust your attitude."

Listening to them, you begin to realize that from launch to landing, everything is carefully planned because where you launch is not where you will land. Skills are important, but so is common sense. Weather is a primary safety consideration, as are power lines, livestock and people on the ground. Selecting a safe place to land and obtaining permission to land, requires tact and diplomacy, and all balloonists are serious about good landowner relations.

A licensed commercial and instructor balloon pilot, Toney cheerfully offers to take you up for free...then somberly tells you that he only charges for the ride down. Julie, as crew chief, now spends most of her time on the ground. "I often flew in New Mexico but am quite satisfied to stay on the ground as crew chief here," she smiles.

Toney suddenly gets serious when he tells you how the balloons are rated aircraft that must be FAA certified; how pilots must also be rated by the FAA; and how the pilot is responsible for everything in the air and the crew on the ground. Julie is equally serious about the crew chief's responsibilities, such as the planning for launches and managing the chase vehicle, crew, radios and other equipment to ensure it's there when the pilot and passengers land. It doesn't seem to matter to her that her job means less time in the air and more time on the ground. Ask them which job is more important and they both remind you that launching and flying a balloon is a team effort.

A balloon ride can last from 15 minutes to over 2-1/2 hours, and usually occurs in a "real wicker basket," Toney explains, "because it's historically the best and the most forgiving material for the purpose. The double-rip-stop nylon balloon fabric with special coatings doesn't require much actual maintenance," he adds. However, the FAA requires an inspection of the aircraft annually or every 100 heated hours by an FAA-approved inspection station. Measurement of fabric porosity and tensile strength are done as well as complete inspection of balloon envelope, flight hardware, and hull (baskets and tanks). A balloon system must "pass" this annually in order to continue flying.

Julie and Toney both say the experience, once airborne, is extremely serene. They describe a quiet that "clears the head," where the only thing you might hear are the occasional sounds of heat gushing from the burners. Julie loves to talk about wildlife she's seen moving on the ground. Toney talks about peacefully floating with the air, about being pushed by the wind but not having any sense of it, about moments of feeling that time had been somehow been drastically slowed.

Just as there is etiquette on the ground, there is etiquette in the air. "The balloon beneath you has the right of way," said Toney. "After all, he can't see up."

Unless you live in the Southwest, cold, wet weather often narrows the Southeast's optimal yearly window for balloon flight. Not much flying is done in the Southeast between November and April due to the cold and wet weather. After all, there aren't many places to hang up a 10-story balloon to dry, Toney explained.

According to the Hansons, there are only about 12-15 other licensed balloon pilots in the northern Alabama area. "There are probably more flying in the Decatur area than Huntsville," Julie said.



© Permission Granted. Photo by Lairy Graves/Danville Commercial-News

(In front) Toney Hanson pilots his hot air balloon, *Sun Dog*, at the Balloon Classic in Danville, Ill. An armada of 63 hot-air balloons participated in the event.

Flying around Huntsville is constrained by mountains to the east, the river to the south, and the Arsenal and airport to the west. It's a lot more fun to do flights out of the city, out near Harvest, so we can get more than one hop."

The Hanson balloon saga began 23 years ago, in Albuquerque, where 30-50 balloons in the sky on a weekend was a normal sight. Julie was working for the Air Force Weapons Laboratory at Kirtland AFB and Toney was in the Navy. First, Tony volunteered to be crew chief on the Navy Balloon recruiting team headquartered at Kirtland AFB, and then he learned to fly one of his own. The couple took a few hot air rides, got hooked, and have been balloon owner/operators ever since.

The Hansons have flown in balloon rallies all over the West, South-east, and Midwest with balloons numbering from 15 to almost 1,000 at "The Big One" in Albuquerque each October. Last June, the Hansons took part in the Balloon Classic in Danville, Ill. There, an armada of 63 hot-air balloons rose up from the county airport in 6-8 mph winds. There are both fun flights and competition at these events and balloons are usually sponsored by local companies or individuals.

Competitive events range from converging navigational tasks (CNTs) like key grabs for new vehicles, money, or even a house to throwing baggies (bean bags) at "Xs" laid out on the ground to see how close you come and garner points toward possibly becoming the overall winner for the event.

"For about the cost of a good fishing rig with a boat and trailer, anyone can take up ballooning," Toney said.

"Becoming a licensed balloon pilot takes persistence and a love for safe flying."



Photo courtesy of the Hansons

Julie and Toney Hanson work at getting their hot air balloon ready for flight. Julie and her husband have spent nearly 23 years enjoying the relaxing views and the solitude of flight. Toney is a licensed commercial pilot and instructor. Julie is satisfied keeping her feet on the ground as the crew chief.