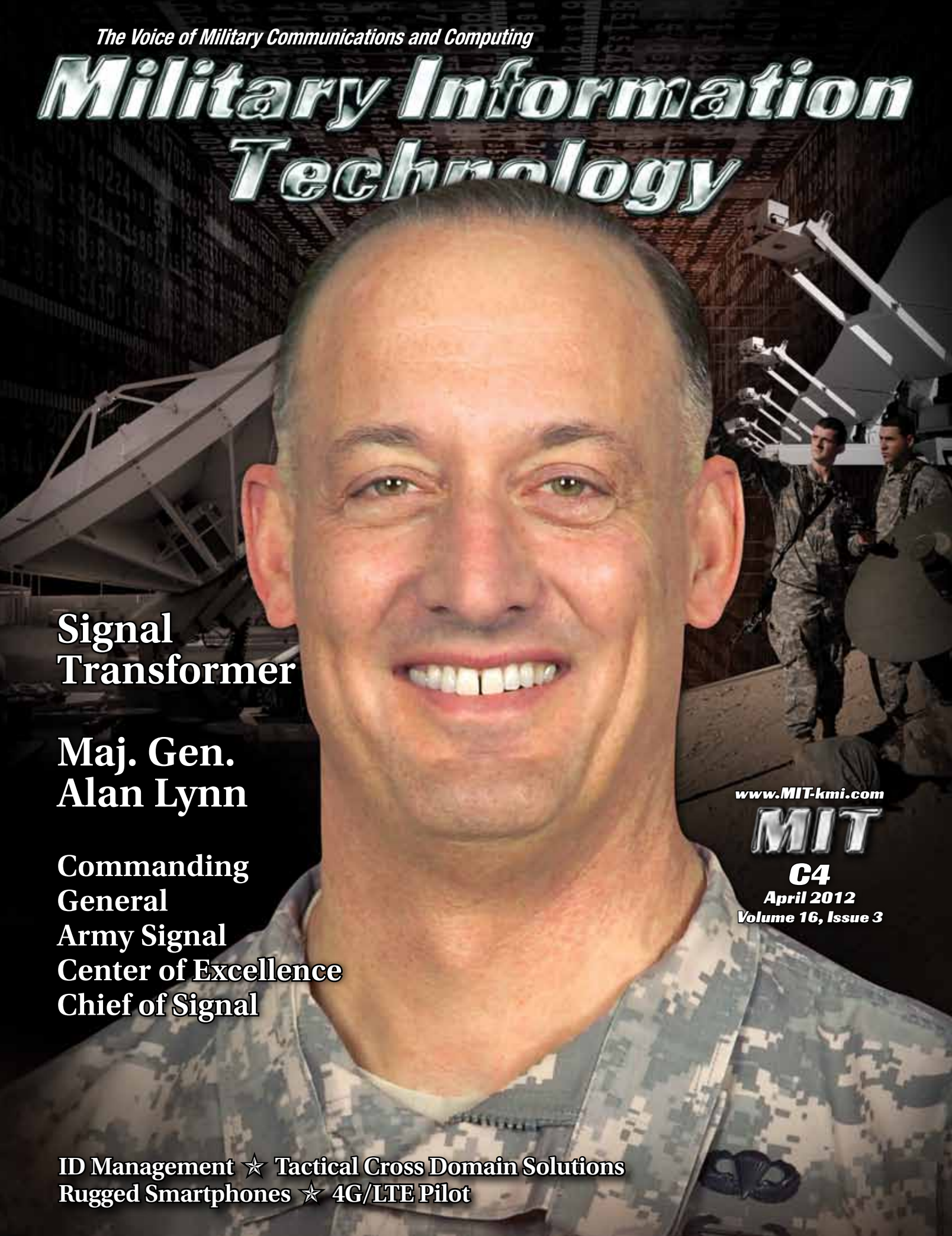
The Voice of Military Communications and Computing

Military Information Technology



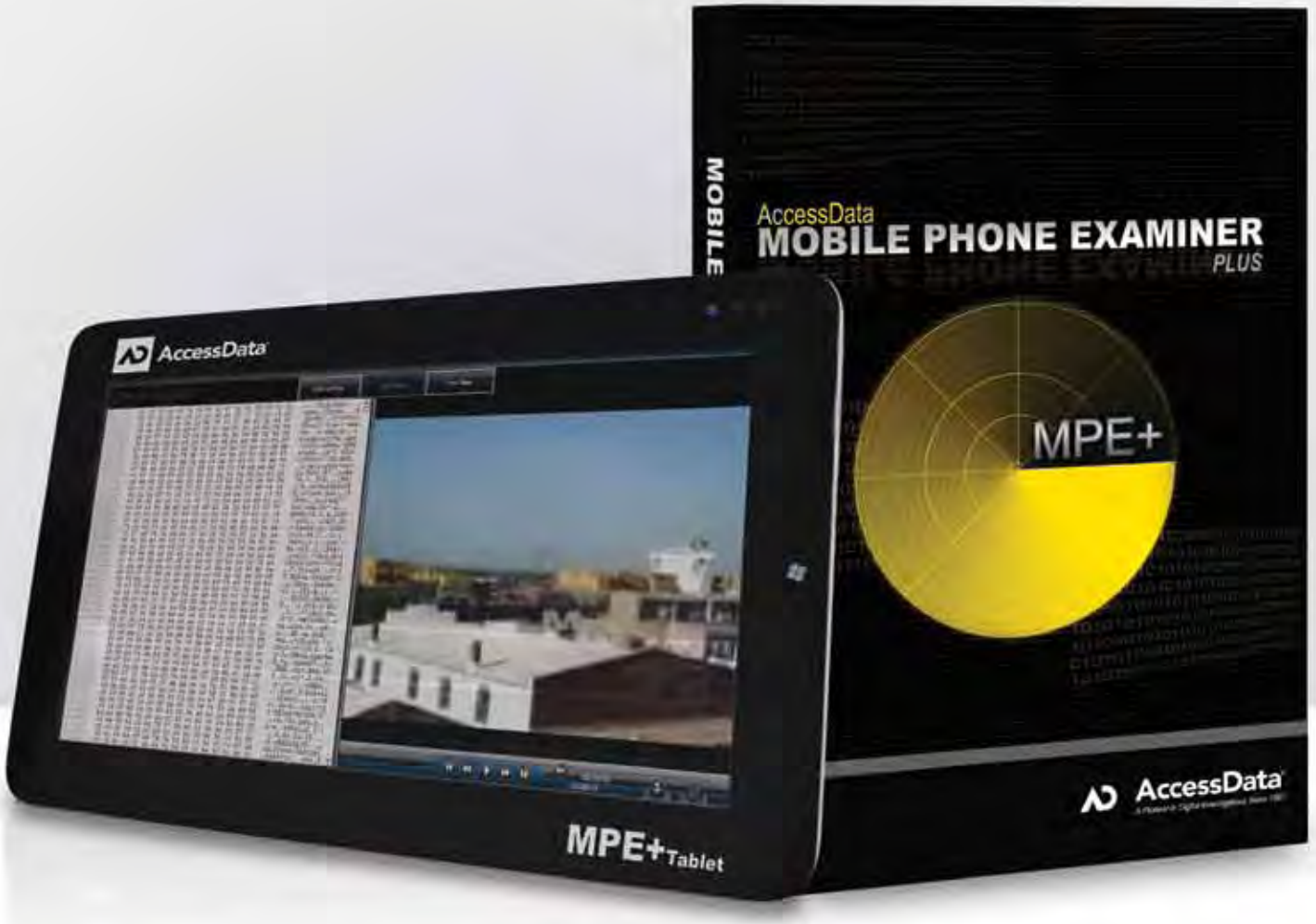
Signal Transformer

Maj. Gen. Alan Lynn

Commanding General
Army Signal Center of Excellence
Chief of Signal

www.MIT-kmi.com
MIT
C4
April 2012
Volume 16, Issue 3

ID Management ☆ Tactical Cross Domain Solutions
Rugged Smartphones ☆ 4G/LTE Pilot



DEVICE SEIZURES GETTING YOU DOWN?

GET MOBILE PHONE EXAMINER *PLUS* FOR JUST $840.*

Replace your common mobile forensics solution with MPE+ to achieve an uncommon digital investigations experience.

Make the switch now...
http://UpgradeToAccessData.com

AccessData

*Offer only valid on mobile device forensics products that retail for $2,000 or more, and annual maintenance fees must be current. MPE+ cable kit and tablet are available separately.

MILITARY INFORMATION TECHNOLOGY

APRIL 2012
VOLUME 16 • ISSUE 3

FEATURES

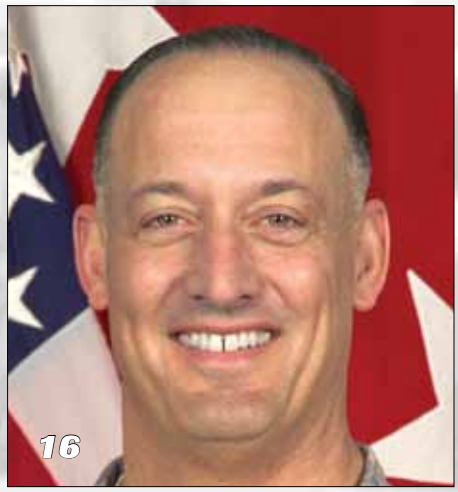
Crossing Domains at the Tactical Edge
The military is pressing for new approaches to tactical cross-domain solutions, which enable warfighters in the field to shift information appropriately and safely between different security levels, and industry is responding.
By Karen E. Thuermer

4G at Sea
Seeking to benefit from the explosive development of capabilities by the commercial smartphone industry, the Navy is launching a pilot project designed to test the effectiveness of the latest cellular technology while at sea.
By Harrison Donnelly

Smart and Rugged
With the increased use of smartphones in the Department of Defense, it was only a matter of time before vendors began offering ruggedized versions.
By William Murray

ID Management's New Challenges
New needs and capabilities are continuing to shake up the world of identity management, particularly as the popularity of mobile computing grows.
By Peter Buxbaum

COVER / Q&A



Major General Alan Lynn
Commanding General
Army Signal Center of Excellence
Chief of Signal

DEPARTMENTS

INDUSTRY INTERVIEW

Thomas Foust
Vice President of Global Network Solutions
Intelsat General Corp.

MILITARY INFORMATION TECHNOLOGY
VOLUME 16, ISSUE 3 APRIL 2012

The Voice of Military Communications and Computing

EDITORIAL

Managing Editor
Harrison Donnelly harrisond@kmimediagroup.com
Online Editorial Manager
Laura Davis laurad@kmimediagroup.com
Copy Editor
Laural Hobbes lauralh@kmimediagroup.com
Correspondents
Adam Baddeley • Peter Buxbaum • Cheryl Gerber
Scott Gourley • Karen E. Thuermer

ART & DESIGN

Art Director
Jennifer Owers jennifero@kmimediagroup.com
Senior Graphic Designer
Jittima Saiwongnuan jittimas@kmimediagroup.com
Graphic Designers
Amanda Kirsch amandak@kmimediagroup.com
Scott Morris scottm@kmimediagroup.com
Kailey Waring kaileyw@kmimediagroup.com

ADVERTISING

Account Executive
Cheri Anderson cheria@kmimediagroup.com
Daniel Call danc@kmimediagroup.com

KMI MEDIA GROUP

Publisher
Kirk Brown kirkb@kmimediagroup.com
Chief Executive Officer
Jack Kerrigan jack@kmimediagroup.com
Chief Financial Officer
Constance Kerrigan connik@kmimediagroup.com
Executive Vice President
David Leaf davidl@kmimediagroup.com
Editor-In-Chief
Jeff McKaughan jeffm@kmimediagroup.com
Controller
Gigi Castro gcastro@kmimediagroup.com
Administrative Assistant
Casandra Jones casandraj@kmimediagroup.com
Trade Show Coordinator
Holly Foster hollyf@kmimediagroup.com

OPERATIONS, CIRCULATION & PRODUCTION

Circulation & Marketing Administrator
Duane Ebanks duanee@kmimediagroup.com
Data Specialists
Rebecca Hunter rebeccah@kmimediagroup.com
Tuesday Johnson tuesdayj@kmimediagroup.com
Raymer Villanueva raymerv@kmimediagroup.com
Summer Walker summerw@kmimediagroup.com
Donisha Winston donishaw@kmimediagroup.com

KMIMEDIAGROUP
A PROUD MEMBER OF

SUBSCRIPTION INFORMATION
Military Information Technology
ISSN 1097-1041
is published 11 times a year by KMI Media Group.

Military Information Technology is free to qualified members of the U.S. military, employees of the U.S. government and non-U.S. foreign service based in the U.S.

All others: $65 per year.
Foreign: $149 per year.

Corporate Offices
KMI Media Group
15800 Crabbs Branch Way, Suite 300
Rockville, MD 20855-2604 USA
Telephone: (301) 670-5700
Fax: (301) 670-5701
Web: www.MIT-kmi.com

EDITOR'S PERSPECTIVE

Harrison Donnelly
EDITOR

Security experts believe that one of the vulnerable aspects of an information system is the supply chain of hardware and software that goes into it. The explosion in use of commercial IT technology by government agencies, as well as the spread of computer component manufacturing all around the world, has created many potential threats to the confidentiality, integrity and availability of critical networks.

According to a recent Government Accountability Office (GAO) report, threats to the IT supply chain can include installation of hardware or software containing malicious logic, counterfeits, production or distribution disruptions, or unintentional vulnerabilities.

This isn't a new issue, and federal law already requires agencies to develop policies and standards for managing supply chain risk. But what really caught my eye in the recent GAO report, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks" (GAO-12-361, March 23, 2012), was how the Department of Defense has been out in front of this issue compared with other key departments.

Looking at the departments of Justice, Energy and Homeland Security, the report found significant shortcomings in addressing IT supply chain risks. Energy and Homeland Security have not defined supply chain protection measures, and while Justice has done so, it lacks the ability to monitor compliance or effectiveness.

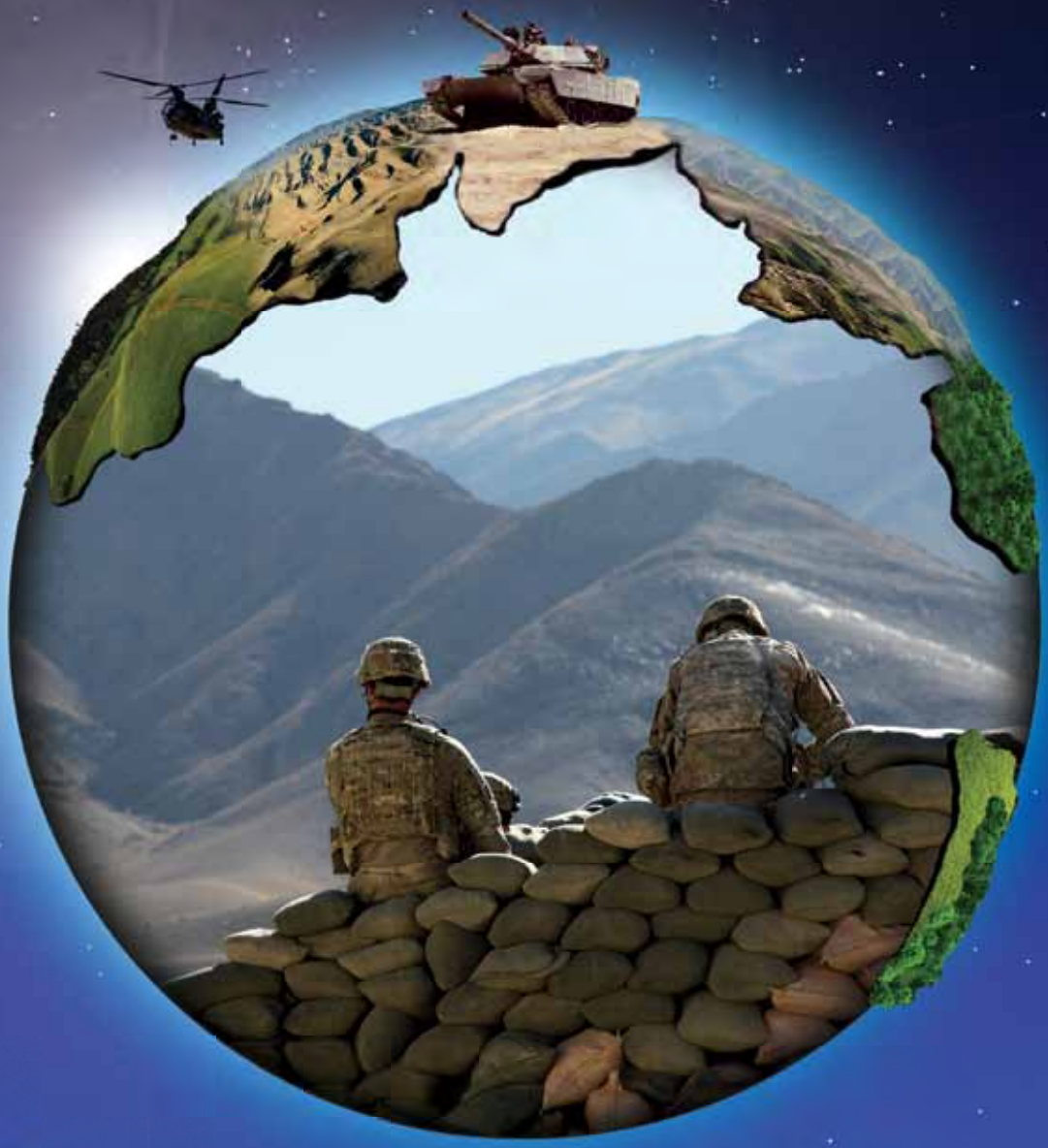
DoD, by contrast, has been working on this issue for nearly a decade, issuing clear standards and establishing monitoring mechanisms. A 2010 guide, for example, lists 32 steps for improving supply chain protection, including maximizing visibility into suppliers and choosing programming languages and tools that counter weaknesses.

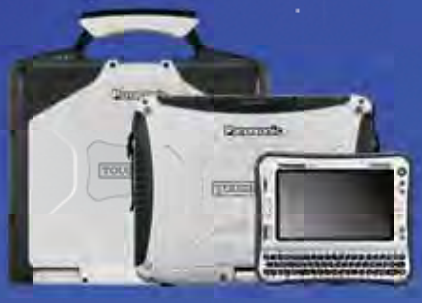
One area in which DoD is similar to the other departments, however, is in not being able to track how much foreign-developed equipment or software their networks contain. But that may not be worth the effort, since intelligence officials believe that a company's relationship with a foreign military or intelligence service is a more reliable indicator of risk than whether a product was manufactured outside the U.S.

Panasonic
ideas for life

intel inside
CORE i5 vPro

Panasonic recommends Windows® 7.





Toughbook 31 Toughbook 19 Toughbook U1 Ultra

Access mission-critical information anywhere. Fully-rugged Panasonic Toughbook® mobile computers, powered by the Intel® Core™ i5 vPro™ processor. Keeping you combat-ready with industry-leading reliability is how we're engineering a better world.

panasonic.com/business-solutions

TOUGHBOOK®

SOLUTIONS FOR THE U.S. MILITARY

PROGRAM NOTES

Compiled by KMI Media Group staff

High Frequency Satellite Terminal Advances

A satellite terminal system for the Air Force that provides protected communications to warfighters has received a successful Milestone C decision and subsequent production award.

The Minuteman Minimum Essential Emergency Communications Network Program Upgrade (MMPU) is Raytheon's first Advanced Extremely High Frequency (AEHF) terminal for the Air Force to enter into the production phase. In another achievement, it became the company's third AEHF terminal to interoperate with the on-orbit AEHF satellite, joining the Army's Secure Mobile Anti-Jam Reliable Transportable Terminal (SMART-T) and the Navy Multiband Terminal (NMT).

The first AEHF satellite, launched in August 2010, recently began an extensive set of operational tests. In this testing, MMPU, SMART-T and NMT demonstrated interoperable communications using the AEHF satellite's eXtended Data Rate (XDR) waveform, moving data more than five times faster than previous EHF systems.

MMPU adds essential nuclear command and control capabilities to the Raytheon AEHF terminal product line established by SMART-T and NMT.

Raytheon is projected to deliver 67 MMPU AEHF terminals, including spares, to the Air Force. The MMPU AEHF systems incorporate Raytheon's XDR waveform hardware and software, including new cryptographic algorithms for protecting national command and control (NC2) networks. XDR and the cryptographic algorithms provide increased bandwidth, speed and significantly improved security within the NC2 communications architecture.

JTRS Office Approves New Software Architecture

The Joint Program Executive Office Joint Tactical Radio System (JPEO JTRS), with participation from the Wireless Innovation Forum, has approved the next generation Software Communications Architecture as SCA 4.0. The first SCA release was in 1999 and since that time several generations of software defined radios have been powered and enabled by this 'operating system for radios.'

SCA 4.0 introduces new technology that tailors the operating system size specifically for the radio and its mission. With this update, memory and processing overhead can be reduced to negligible levels, and architectural enhancements can improve security by enabling much faster boot-up times and reconfiguration of the radio.

The power and flexibility in the SCA enables reprogrammability of radio frequencies, and because it is open architecture, permits a waveform written for one radio to be ported readily to another radio. This capability allows governments and organizations to develop a waveform once and then reuse the waveform on multiple radios, with the assurance of interoperability.

Government and military radios have much longer lifetimes than the two years of today's commercial products. SCA 4.0 is specifically designed for the reprogrammability of the radio frequency and signal processing components so the radio can be upgraded with a software download anywhere it is installed.

PEOPLE

Compiled by KMI Media Group staff

Air Force **Lt. Gen. Charles R. Davis** has been nominated for appointment to the rank of lieutenant general and for assignment as military deputy, Office of the Assistant Secretary of the Air Force for Acquisition. Davis is currently serving as the commander, Electronic Systems Center, Hanscom Air Force Base, Mass.

Regina Dugan, who has served as director of the Defense Advanced Research Projects Agency for the past three years, has accepted a senior executive position at Google.

The Army Communication-Electronics Command has officially welcomed its 20th commander, **Maj. Gen. Robert S. Ferrell**, who will also serve as installation commander of Aberdeen Proving Ground, Md.

Allen Greene

HP has appointed **Allen Greene** as vice president of Department of Defense sales. In this newly created position, Greene will report to **Tom Hempfield**, vice president, U.S. Federal Organization, HP. Greene will manage the global DoD business for HP, including the Defense Information Systems Agency, Air Force, Army and Navy.

General Dynamics has selected **Phebe N. Novakovic** to be the corporation's president and chief operating officer reporting to **Jay L. Johnson**, chairman and chief executive officer.

Bob Rowe

TrustComm Inc., a global provider of secure satellite communications services, has made significant changes to its senior management team as part of its renewed focus on providing customized solutions for the Department of Defense. The company appointed satellite industry veteran **Bob Roe** as its new chief executive officer. Roe served for more than five years as CEO of Stratos Government Services Inc. In addition, **Ian Canning** has been appointed chief operating officer of TrustComm.

Stu Shea, president of SAIC's Intelligence, Surveillance and Reconnaissance (ISR) Group, has been named chief operating officer of the company. **Tony Moraco**, who has been serving as executive vice president for operations and performance excellence, has replaced Shea as president of the ISR Group.

WHEN SECURITY IS CRITICAL.

Securing information from point to point and throughout your network — when it's critical, it's QinetiQ North America.

Your cybersecurity challenges require innovation to identify risks and eliminate threats. We have the capabilities, the credentials and the mission success to deliver it.

Discover where innovation lives at **www.QinetiQ-NA.com/GetSecure**

WHEN IT'S CRITICAL, IT'S QINETIQ.

QinetiQ
North America

Crossing Domains
at the Tactical Edge

Army seeks lightweight, field-ready systems for transferring information at different levels of security.

By Karen E. Thuermer
MIT Correspondent

As military theory and practice increasingly push data to the tactical edge and encourage sharing it at all levels, warfighters in the field need more than ever to be able to shift information appropriately and safely between different security levels.

There is no shortage of technology, known as cross-domain solutions, for regulating that transfer of data between secrecy classifications. But such systems generally are designed for networks based in stationary facilities located far from the battlefield, where considerations of size, weight and ruggedness are less demanding.

As a result, the military is pressing for new approaches to what are called tactical cross-domain solutions (TCDS), and industry is responding.

William Cannon

bill.cannon@advatechpacific.com

One strong sign of the importance of TCDS came recently from the Army System of Systems Integration Directorate, which asked interested industry and government sources with mature solutions to enhance existing network systems capabilities to participate in a Network Integration Evaluation event. Its purpose was to find solutions with a narrow focus on specific identified gaps in the current and evolving networked equipment solution set.

Among the identified "gaps," or product needs, were tactical cross-domain systems that are low in cost, weight, size and power consumption.

The Army is finding that TCDS is increasingly critical since the demand for sharing situational awareness data at the tactical edge is growing. This growth is due in large part to the nature of the asymmetrical warfare the U.S. has encountered in last decade, and the increasing trend to operate with joint coalition forces even at the small unit level.

Army and Marine Corps leaders have embraced the value of providing these front-line soldiers with timely, accurate and relevant situational awareness information.

"They recognize how it will literally save lives and amplify the fighting power of U.S. troops, since it arms them with the knowledge of where the enemy is, what he is doing, and where their friendly forces are in support of them," said William Cannon, director, Electronics and Communications Business Unit for Advatech Pacific.

The need for joint and coalition ground forces in Iraq and Afghanistan to securely share information among operators at the tactical edge makes this particularly evident.

"Secure information sharing no longer is imperative only agency-to-agency or peer-to-peer," commented Rich Stankevich, marketing manager for Owl Computing Technologies. "Command post- and vehicle-secure data are just as vital as building-secure data. Downsizing and ruggedizing those transfers, even to the individual warfighter, are the challenges."

Optimized for the Edge

Warfighters at the tactical edge have a critical need to exchange information between units, especially since units access information at varying security levels.

"For those reasons, cross-domain solutions optimized for and deployed at the tactical edge are becoming more important," said Mike Parry, director of business development for DRS Defense Solutions.

Consequently, the move over the past decade has been to push cross-domain technology and capability into small form factor (SFF) footprints to address the size, weight and power (SWaP) constraints and to provide increased accessibility to that technology and capability for the warfighter in the field.

"As a result, there are now more available platforms that can support limited cross-domain technology and capability, yet the limitations imposed on that implementation of technology and capability are constraining the warfighter and associated command structure from establishing and maintaining a broad assured information sharing environment," remarked Shawn Campbell, director of government solutions at SafeNet.

An example of the impact of those limitations is that the current and near future SFF systems support information sharing environments involving just two security domains—secret and unclassified.

Shawn Campbell

shawn.campbell @safenet-inc.com

Aaron Maue

Mike Worden

Tim Goodrich

"In today's overall operating picture, there can be a number of security domains, such as coalitions, nongovernmental organizations and communities of interest, that all participate in the operational environment and its information sharing environment," he said. "The current SFF cross-domain solutions are unable to allow the warfighters and their command structure to participate in that broader assured information sharing environment."

The challenge is that some of the information generated by U.S. forces has to be sanitized before sent to coalition partners, and TCDS often have to connect dynamic tactical networks rather than bridge the traditional NIPRNet, SIPRNet, and Joint Worldwide Intelligence Communications System networks.

"Those tactical operators often cannot rely on reachback to enterprise CDS because of intermittent connectivity from the core to edge, unacceptable latency introduced by reachback to the core, and the semi-rigid nature of enterprise CDS policy implementations," said Parry.

Thanks to advancements in TCDS, however, information can be exchanged between units and shared digitally instead of by voice. "This makes situational assessment more accurate and complete and less prone to human communication errors," Cannon added.

And while TCDS technology can not yet address units as small as an individual soldier or Marine, it does operate at the platoon level and is moving down to the squad and fire team level.

Challenging Development

The technology has not been easy to develop. The tactical edge environment itself places great challenges on TCDS.

"Solutions in the tactical environment must stand up to much more stringent environmental conditions, including rain, salt, dust, vibration and extreme temperatures," commented Aaron Maue, programs manager, open and cross-domain solutions, Rockwell Collins.

Another challenge is physical requirements for TCDS. Tactical implementations require that TCDS technology must be small and as lightweight as possible, yet powerful enough to deliver trusted usable information.

"A group of characteristics is the size, weight and power of any equipment to be used at the small unit level, whether in a vehicle or on an individual soldier," Cannon explained. "Both have critical SWaP constraints, especially the dismounted soldier who has to carry his equipment load (typically 85 pounds or more) through all kinds of physically challenging environments."

To be effective, TCDS footprints are generally reduced to be able to be integrated into aircraft, submarines, HMMWVs and other platforms that face space constraints.

"In the airborne environment, in particular, cross-domain solutions often must pass safety certifications in addition to security accreditation," Maue added.

Since TCDS often reside in ground and/or air platforms, they also need to meet demanding environmental certifications. As a result, SFF solutions are required to emphasize SWaP requirements and often military standard ruggedization, as well as environmental cooling requirements.

"Cross-domain solutions running on a single-board computer can provide all the functionality a customer needs while also providing savings in space and weight required by a small platform such as a drone," said Mike Worden, director of integrated intelligence solutions, Lockheed Martin.

In most other applications, CDS can be installed on servers in buildings that have plenty of space and can easily scale up if necessary. Whereas a tactical solution would have targeted information flows, an enterprise environment would be better suited to new data streams and multiple channels of data flow.

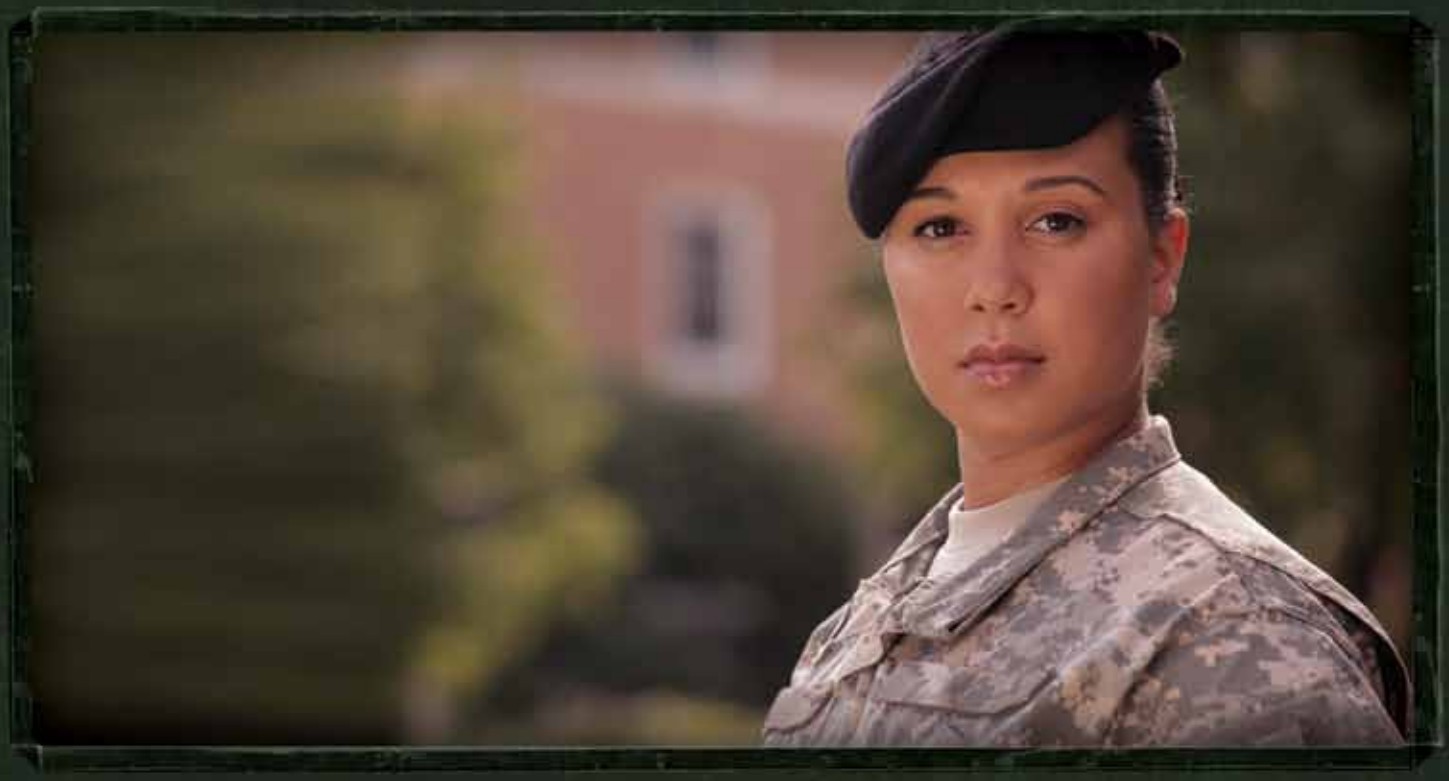
Another issue consideration is training, noted Tim Goodrich, president and chief executive officer of Timitron Corp., a provider of TCDS solutions and services. "One of the most relevant issues with any innovative, new solution is training. TCDS training must be flexible enough to be pushed down to the lowest level of warfighter utilization. To take the tactical user from the war to train up and equip with a TCDS solution is not a feasible option. Training on such TCDS platforms must meet requirements that support organization training at the unit level," stated Goodrich.

"We are committed to developing an understanding of key technologies and implementing these solutions in support of the warfighter," he added.

Another key characteristic is the level of ruggedization TCDS devices need to survive the environment extremes of the tactical edge. This is critical, particularly in situations where a TCDS is residing in a vehicle that is damaged by an IED.

"Operational conditions also pose constraints on TCDSs as the potential for catastrophic conditions concerning loss of power, communications and possession is so much greater than data center or enterprise environment," remarked Campbell.

36,000 ACTIVE-DUTY STUDENTS. ON BASE. ON-SITE. ONLINE.



Wherever your mission takes you, anywhere in the world, you'll find University of Maryland University College (UMUC). We offer courses on base or on-site in more than 25 countries—and over 100 bachelor's and master's programs entirely online. That's our mission, because since 1947, UMUC has been educating America's armed forces.

UMUC
University of Maryland University College

AT YOUR SERVICE SINCE 1947

★ University of Maryland University College is the nation's largest public university. ★

877-275-UMUC • military.umuc.edu/servesyou • enroll now

Then there's the issue of security. "If the TCDS is vulnerable to being captured, and therefore venerable to exploitation, there's a possibility that sensitive information could be revealed to our enemies," explained Parry. "Capture would expose TCDS to physical exploitation."


David Bukovick

Consequently, TCDS must be highly tamper resistant, with several layers that essentially erase all information on the device if tampered with. Since tactical end-user devices are more likely to be at risk of physical loss or compromise, capabilities have to include features that would prevent unauthorized users from accessing classified information.

Another big issue facing this technology is the speed at which it can be deployed to those who need it.

"Because of the time it takes to tailor most of the available solutions to the requirements of the given platform and then to accredit it for use on that platform, there is a significant delay in fielding solutions to the warfighters," Maue explained.

Certifying and obtaining accreditation for TCDS through the National Security Agency is a lengthy process. "It normally takes 18-24 months to get a new device through this process, and it's an expensive undertaking requiring a government program sponsor to initiate and support the process through to completion," remarked Cannon.

Another major challenge for the technology is its integration into existing platforms. Because security measures typically have to be designed into platform architecture from the ground up, it can be very difficult to integrate a cross-domain solution into a tactical platform architecture after that platform has already been fielded.

Last but not least is the issue of cost. "Due to the large number of small units (vehicle and dismounted), the equipment not only has to be small, light and power efficient, it must be relatively cheap—at least two orders of magnitude cheaper than the cross-domain solutions fielded at the command centers," Cannon said.

While processing information as secret on the tactical warfighter level is paramount, one of the most difficult issues is the dramatic increase in the cost of its deployment.

"If an organization can deploy a resource, such as a warfighter, vehicle or aircraft, that does not require a high security classification, its deployment will be less costly," said Stankevich. "That resource can transfer field information into a higher security enclave in real time, with minimal risk, via some form of TCDS, and receive actionable direction."

In other words, the field deployment of information becomes much more cost effective if a point of information collection and reception is provided at a lower level of security and is either effectively transmitted to a higher level of security or disseminated down while maintaining that information at a high security level and protecting the networks over which it is being traversed.

Addressing the Need

Numerous contractors are addressing the challenges associated with TCDS and offering various platforms. According to Dave Bukovick, program manager for multi-level and cross-domain solutions for General Dynamics, the commercial sector is releasing a new generation of user devices roughly every nine to 12 months. "We have to keep up with that latest technology while, at the same time, making sure that each new generation provides greater capability to warfighters without compromising security," he said.

Among the TCDS products General Dynamics offers are CrossingGuardXD, which is used in virtualized environments; TacGuardXD, which resides on a single board for deployment in multiple tactical platforms; and NanoXD, which is an ultra-small guard product that is a component of equipment like the GD300, a rugged wearable computer that is used by dismounted military personnel.

"NanoXD can be used to mediate data transfer between one network of soldiers and another, sharing valuable location information," Bukovick explained.

General Dynamics is also advancing cross-domain security in the cloud with its Trusted Network Environment (TNE) product. Built on a foundation of COTS products, TNE allows users to access, share and fuse information across security domains in a cloud environment.

The Guard products use ruggedized COTS computing platforms, which lowers lower cost and makes for easy integration.

Bukovick pointed out that General Dynamic's cross-domain solutions can be configured to the needs of any program. The company is also working to make information sharing as "device independent" as possible.

One of the advantages of General Dynamics's TCDS products is that they have been designed to address concerns like weight and power consumption, so less space is used on technology and batteries and more is available for weapons, ammunition and other needs.

"We also ensure that our solutions are integrated so there is no user interaction or training required," Bukovick added.

SafeNet's Multi-Domain eXchange (MDeX) system is capable of supporting both enterprise and tactical information sharing environments. It was designed and built to share releasable information safely between organization, international, information and security domains.

Exchanges are done with authorized recipients so that the correct data gets to the correct place in the right amount of time.

"With its inclusion on the Unified Cross Domain Management Office (UCDMO) baseline, it is available for reuse among intelligence community, DoD and partner organizations," Campbell said, adding that the fact MDeX is on the UCDMO baseline for approved operational government use makes the system unique.

Additionally, the MDeX System's modular design permits a software CDS edge interface for direct warfighter accessibility to cross-domain technology and capability, while the CDS itself remains better protected within fielded vehicles.

"This reduces some of the risk of exposing core CDS technology and capability in the open environment," Campbell said.

Lastly, by addressing SWaP, but not being exclusively driven by that requirement, the MDeX System CDS can support an assured information sharing environment across multiple security domains, such as U.S.-secret, coalition-secret, NATO-unclassified and U.S.-unclassified, to provide a common and complete operating picture for both the warfighters and their command structure.

MDeX also offers a complete remote management station that provides an intuitive graphic user interface for complete remote management, policy configuration management, and to view audit, system and application events.

"This user-friendly design enables systems managers to quickly learn MDeX System operations," Campbell said.

SafeNet's MDeX System was built with a modular design to concurrently support multiple types of protocols, data, content filters and security domains without changing its core CDS capability. This makes it possible to connect to partner infrastructures and share almost any type of information, without engaging in extensive reassessments of the core CDS capability. This reduces the time from mission need to mission operation from many months or years to weeks or a few months.

Automatic Sanitization

Lockheed Martin provides two solutions, Radiant Mercury and TMAN, that seek to satisfy an extremely varied range of requirements. Radiant Mercury addresses automatic sanitization of highly structured data, while TMAN addresses high speed streaming data products.

"These two products evolved over time to satisfy complementary requirements and are highly configurable to meet the varied requirements of a diverse customer base," said Worden.

TMAN has a SFF system with hardware requirements that will support high altitude systems at 65,000 feet. "This high altitude TMAN solution was developed to support UAVs with streaming video and Link 16 data flowing in both directions," Worden described.

The entire TMAN system supports four separate security domains, ensuring proper dissemination of data to each domain.

Owl Computing Technologies has a product now identified within the CDS community as OCDS-ST01. It is an in-theater CDS supporting the transfer of real-time video and meta-files. In this instance, the secure all-digital transfer of FMV provides higher resolution (and more support data) than FMV "scrubbed" via an A-D-A conversion.

"We have a number of tactical CDS variants—full-blown dual-server instances and single-chassis implementations," commented Stankevich.

What sets its product apart is its re-usable modularity. In addition, he explained, Owl delivers CDSs directly addressing user need, at known cost, with life cycle management. "And because the CDS accrediting community knows our solutions, new implementations reach accreditation and operational deployment sooner, at lower cost," he added.

DRS Defense Solutions offers three products under TCDS: its first and currently certified and employed Diamond Back Guard, Diamond Back Guard Plus, which has been delivered and is currently undergoing testing, and a system it is now developing that the company believes will be a significant leap ahead, Python Guard TCDS.

"To our knowledge, this is the first TCDS that introduces trusted computer elements," Parry said.

What sets Python Guard apart is its trusted architecture that protects against physical and digital attacks. Python also provides extremely high performance in a small package at a very competitive price. Python is small, powerful and draws limited power, yet introduces a verifiably secure separation architecture on a single high-performance chip. Python Guard is also self-aware and self-protecting to counter the unique threats at the tactical edge.

Python Guard focuses on the tactical data message and file types typically exchanged by operators at the tactical edge.

"Python Guard can be used to sit between tactical networks, for example, and mediate secure cross-domain Variable Message Format (VMF) message exchange between different security domains," Parry explained.

Meanwhile, Advatech Pacific claims that its TACDS is the first TCDS designed to meet all of the SWaP, environmental and information assurance requirements for devices intended to be used at the small unit level, first in tactical vehicles and then down to dismounted soldiers.

"We have used the latest single chip field programmable gate array technology with dual core embedded processors to reduce the SWaP to a very small footprint," Cannon explained. "At the same time, we have developed a rigorous security architecture utilizing the latest NSA cross-domain and single-chip crypto technology guidance, and then incorporated strong, multi-layered anti-tamper mechanisms into it."

The unit was designed from the ground up to address all of the risk factors identified in NSA's risk decision authority criteria, and includes strong, reactive mitigation approaches to each of the factors identified in that guideline. This approach led to TACDS achieving a low technical risk rating during Advatech's security design review last fall with NSA, only the second CDS to achieve that rating.

Advatech describes TACDS as a rule based, bi-directional guard that filters the content of message traffic in real time, requiring no "man in the middle."

"We are currently certifying the device with a VMF filter component," Cannon added.

TACDS is built to handle the environmental extremes of tactical wheeled and tracked vehicles, including the shock effects of gunfire recoil. It also has a highly secure, componentized architecture including secure boot, role based administrator authentication, and FIPS 140-2 Level 4 tamper resistance.

"We also provide a graphical user interface tool called Stride for creating these XML files, which can be downloaded into the device through a separate management port available for administrator access," Cannon explained.

Connecting Warfighters

Rockwell Collins's TCDS offerings range from soldier-wearable solutions to those that can be integrated into various fixed and rotary wing aircraft as well as vehicle platforms.

"Our soldier-wearable MicroTurnstile cross-domain guard weighs only a few ounces and operates on less than one watt of power," described Maue.

It provides a warfighter the ability to connect his classified computing device (wearable computer or smartphone) to his unclassified handheld radio. "By enabling these two devices to connect to one another, he is able to view the location of all of the members of his squadron on the moving map shown on the computing device," Maue said.

According to Maue, MicroTurnstile provides the lowest weight, lowest power soldier-wearable cross-domain guard available.

Rockwell Collins's SecureOne Cross Domain Technologies product line provides a low-SWaP solution to process, display, store and transfer data at multiple classifications levels by including the SecureOne Processor, SecureOne Guard, SecureOne Network, SecureOne Display and SecureOne Storage.

The SecureOne Guard product can be implemented on a platform to allow an uncleared aircraft maintainer to download fault log and usage data from a system that contains classified information. "Without the SecureOne Guard, the maintainer would need to be cleared to the highest level of data that is processed by the system," Maue added.

An added plus, the SecureOne solution takes advantage of open standards to enable a minimally invasive implementation on most tactical platforms. "Through the use of these open standards, we can build a system from the ground up or use a platform's existing infrastructure to deliver secure solutions," Maue said. Another leading company in the field is Raytheon Trusted Computer Solutions (RTCS), which has been involved with CDS for over 15 years. The company has the most approved products on the UCDMO base line.

"It's all we do," commented Ed Hammersla, chief operating officer of RTCS. "Most other companies' main business is cybersecurity. They do CDS as a specialty offshoot."

Among RTCS's products are its Trusted Gateway System (TGS), Trusted Thin Client (TTC), Trusted Thin Client (TTC), SimShield, and WebShield.

"These are used in the various ways DoD tactically shares information," Hammersla stated.

TGS acts as "the man in the loop," Hammersla explained. It secures multi-directional data transfer by providing built-in manual review and automatic validations, which enables safe and simultaneous data movement between networks at different sensitivity levels.

TTC secures access to multiple domains from a single connection point. HSG offers automated, high performance data transfer, enabling highly complex bi-directional, automated data transfers between multiple domains.

"SimShield is used for training and simulation work," he continued. "And WebShield is a COTS data guard that provides secure web search and browse-down capabilities from high speed networks to lower level networks."

All five of these products are approved on the UCDMO base line reuse list. "They are the most widely deployed cross domain solutions," he said.

Future Directions

The future holds many challenges for TCDS. For one, such systems will continue to need to address SFF and SWaP requirements.

"But other technologies and operational conditions will continue to pressure tactical CDSs to support much broader assured information sharing environments," Campbell remarked. "Increasing capabilities and bandwidth of network infrastructures will continue to drive the need for tactical CDSs to quickly adapt to higher performance networking and processing platforms while continuing to balance those SFF and SWaP requirements."

Campbell also predicts that as virtualization technology becomes more secure, so that true trusted hypervisors become broadly accepted as providing sufficient assurance for tactical CDS platforms, virtualization technology may be the biggest influence in addressing both SFF/SWaP and expandability/processing requirements for tactical CDSs.

Parry sees TCDS branching in several directions: one in which modules and encryption modules will become more tightly integrated, and another where TCDS will integrate with communications gateways that bridge dissimilar communications networks operating different waveforms, but also operate at security levels.

"The certification and accreditation community will have a large role in the successful deployment of a merged CDS-encryptor device," he said.

Worden predicts that virtual machine technology that will allow CDS to run on hardware shared with other applications will become increasingly important. "Virtual machine CDS will ultimately reduce SWaP concerns and provide superior options for deployment, management failover and scalability," he said.

Bukovick expects that with large test events such as NIE becoming more and more prevalent, in order to rapidly field low-risk, highly mature solutions, the demand for high-quality, cost-effective solutions will increase over the next five years.

"We also see the cross-domain solutions migrating to greater reliance on robust, secure cloud-computing environments, with greater reliance on the cloud for providing security to a broad cross section of ruggedized and commercial devices," he said.

As TCDS solutions continue to grow in their importance, Maue remarked, they will become critical parts of nearly all platform integrations. Besides needing to provide ever-increasing capabilities in smaller and smaller packages, the largest influence on the direction and proliferation of TCDS will be the significant growth in the number of tactical networks that need to be accessed by the warfighter.

"As our servicemen and women rely on these networks to pass everything from voice to real-time video, they will need cross-domain solutions that support transfer, display, processing and storage solutions to keep their missions safe and successful," Maue said. ✭

For more information, contact *MIT* Editor Harrison Donnelly at harrisond@kmimediagroup.com or search our online archives for related stories at www.mit-kmi.com.

4G at Sea

Navy to test the effectiveness of the latest cellular technology on a three-ship expeditionary strike group.

By Harrison Donnelly
MIT Editor

Seeking to benefit from the explosive development of capabilities by the commercial smartphone industry, the Navy is launching a pilot project designed to test the effectiveness of the latest cellular technology while at sea.

Naval Air Systems Command (NAVAIR) plans to undertake a 4G/Long Term Evolution (LTE) pilot aboard a three-ship task force slated for deployment early next year, according to John Cooper, program director, who outlined the project at a recent AFCEA event in Solomons, Md.

When it is configured on the USS *Kearsarge* Expeditionary Strike Group, the 4G/LTE system will use commercial cellular technology to provide intership and intraship communications for the three vessels. Each ship in effect will have its own cell network covering an area of 10-20 nautical miles in diameter. For air platforms, coverage could be available in an area up to 30 miles across.

One example of a use case could involve a helicopter transmitting sensor data through the system to boat crews preparing to board a vessel in search of suspected terrorists.

The Android-based devices in the test will offer typical smartphone capabilities, including video, voice and data and a basic whiteboarding application.

Larry E. Hollingsworth

The pilot project reflects a conscious effort by the Navy to shift the paradigm by which they and the other services develop networks, Larry E. Hollingsworth, national director of AIR-4.5 Avionics Department at NAVAIR, explained in a recent interview.

"Typically, we set up programs of record that go through the DoD 5000.2 process, with milestones A through C, cost hundreds of millions of dollars and take eight to nine years," Hollingsworth noted. "By the time we get through that process to field something, it is usually obsolete with respect to what is on the commercial side.

"We took a look at the commercial market and what they're doing—the five companies that are providing 4G capability—and they along with the major telecommunications companies are spending about $30 billion a year in development. That's more than all of what the Department of Defense spends on developing networks. There is no way we can keep up."

Hollingsworth pointed to projections frequently highlighted by Lieutenant General Susan Lawrence, the Army CIO/G-6, that show a growing gap between the capabilities of consumer technology and those of military systems. The goal, he said, is not to close the gap with the commercial sector, but to eliminate that gap.

"The only way to eliminate the gap is to get on the bandwagon with the commercial market and what they're doing with 4G. Today, you have a cellular device that is probably about 8 megabits capable. In two years, that same device will be able to handle a gigabit, without purchasing another device," Hollingsworth continued. "If I were trying to do that as a government development program, it could take hundreds of millions of dollars and a lot of time, because I'm not spending the $30 billion a year to accelerate the schedule and technology to market. We're trying to leverage that investment, and all of the good things it provides in terms of speed and backwards compatibility."

ISR Capabilities

As for the uses to which the devices could be put on the ships, Hollingsworth and Cooper seem open to the possibilities.

To begin with, the 4G system could provide cellular phone service between members of the expeditionary strike group, provided they were within sight of each other. Another basic service could be video teleconferencing between ships.

But it is the ISR uses of the smartphones, with their video and other data-capture capabilities, that may offer the greatest rewards.

"One of the biggest needs in the battlespace is ISR and movement of relevant information in a timely fashion. In this case, you can have forces on a mission, with an ISR platform overhead, and at best one person in the group may get some information on a Rover device, if the unit is so equipped. But we're talking about giving every warfighter a device by which they have a common operational picture of their mission. Whatever information is being collected by an overhead asset can be given in real time to everyone in the unit," Hollingsworth said.

The pilot program, however, is not expected to provide a device to all enlisted personnel, using instead a combination of individual units and larger video displays on ship.

"When we put this capability in the hands of Marines and sailors, I'm sure they're going to think of many different ways of using this capability that we haven't thought of," Hollingsworth said.

Meanwhile, Cooper reported that work was underway to install the needed equipment on the three ships, which also include the USS *San Antonio* and USS *Carter Hall*. Currently, engineers and developers are studying where to put the antennas on the vessels, whose decks are already crowded with electronic equipment.

Oceus Networks announced in late March that the Navy had selected the company's Xiphos mobile communications networking solution for the pilot. The Xiphos tactical cellular solution will provide high capacity secure wireless broadband for real time access to ISR data for intra-ship communications over the horizon, and inter-ship communications via commercial hand-held devices. ✯

For more information, contact *MIT* Editor Harrison Donnelly at harrisond@kmimediagroup.com or search our online archives for related stories at www.mit-kmi.com.

Task Order Implements Host Based Security System

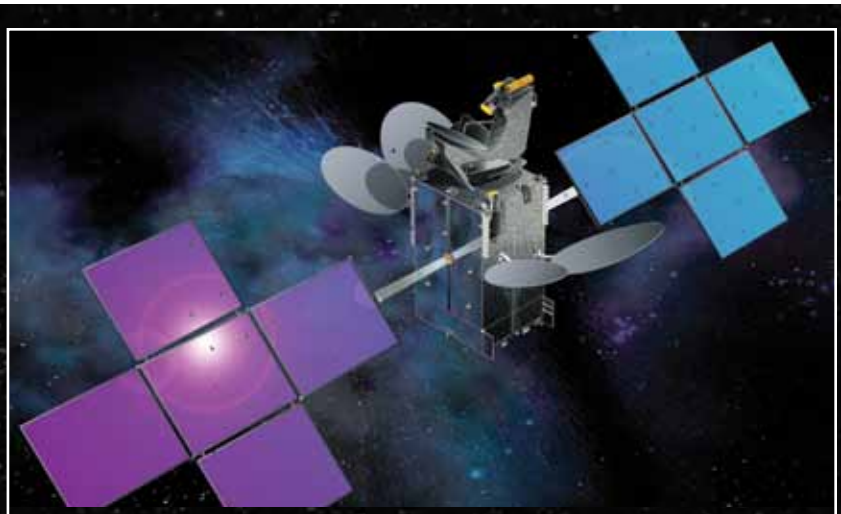
The Defense Information Systems Agency has awarded Northrop Grumman a cybersecurity task order to strengthen cybersecurity protections across all Department of Defense and intelligence community networks by implementing the Host Based Security System (HBSS) as part of the DoD Information Assurance and Computer Network Defense contract. The task order was competitively awarded under the Encore 2 contract vehicle and is valued at $189 million over a three-year base period with two one-year options. As prime integrator, Northrop Grumman will provide software license maintenance support, training, help desk and architectural infrastructure support personnel. HBSS is DoD's COTS suite of automated and standardized software used to provide enhanced host based security—security on desktops and laptops versus at the boundary such as routers and switches—against both internal and external threats. Under the terms of the contract, Northrop Grumman will provide support in architecting, engineering, maintaining, deploying and implementing the HBSS solution. Northrop Grumman's teammates on the contract include McAfee and CDWG.

Collaboration to Provide End-to-End COMSATCOM Services

Artel and Boeing Commercial Satellite Services will collaborate to distribute Inmarsat-3, -4 and -5 bandwidth to potential U.S. government customers. It is anticipated that this first collaboration will be followed by additional offers to provide unique end-to-end commercial satellite services to U.S. government and commercial customers. Boeing and Artel are working with potential customers and users to develop Ka-based satellite communications solutions for their unique applications. Inmarsat-3 and -4 services are available now. Inmarsat-5 global satellite communications will be available starting in late 2013, and users will be able to conduct compatibility testing on their Inmarsat-5 terminals starting in the middle of that year. Artel is the largest provider of commercial satellite communications services to the Department of Defense.

Navy Taps Nine for COTS Equipment

The Navy Space and Naval Warfare Systems Center Atlantic has awarded a contract to provide COTS ISR, information operations and information assurance equipment to the following companies: Atlantic Diving Supply, CDW Government, Global Technology Resources, GTSI, iGov Technologies, Mercom, Science Applications International Corp., Scientific Research Corp. and World Wide Technology. The contracts include options, which, if exercised, would bring the cumulative combined value of these contracts to an estimated $500 million.

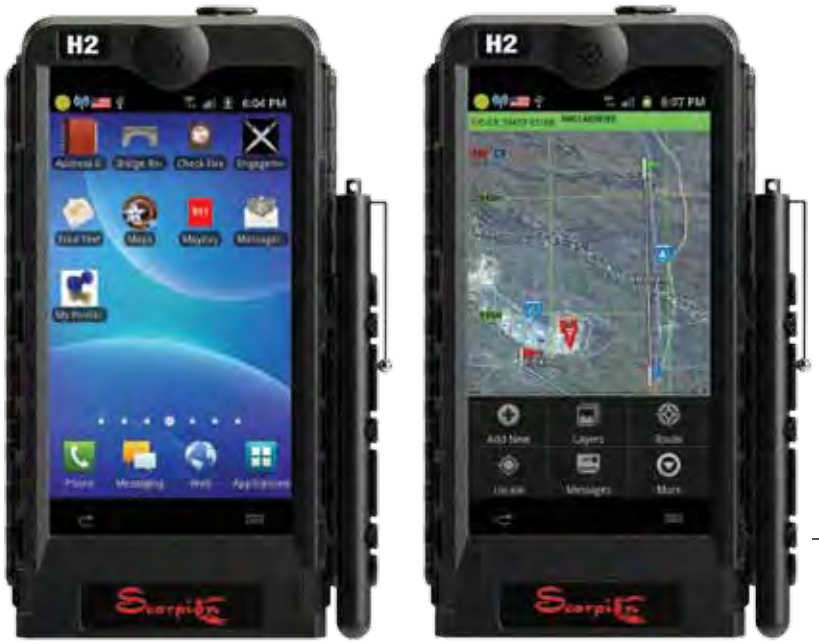


Upgrade Enhances Space-Based Internet Routing

TeleCommunication Systems (TCS) has completed production integration testing and roll-out of a software upgrade to its TCS OS-IRIS offering, which is hosted on Intelsat 14. TCS OS-IRIS is the world's first commercial service offering of a Cisco-enabled IRIS (Internet Routing in Space) managed satellite service. This upgrade adds enhanced encryption and additional IPv6 support to the platform, which already supports seamless, end-to-end Layer 3 IP. By leveraging the upgrades and the benefits of Layer 3 IP routing via satellite, secure, end-to-end IP virtual private network services can be offered with new levels of security, flexibility and network control. TCS is the exclusive commercial services operator of IRIS-enabled satellite services on Intelsat 14, allowing organizations to reach multiple continents from a single connection to TCS' network infrastructure. TCS OS-IRIS allows organizations to directly connect sites on multiple continents without the need for double satellite hops or the traditional connection to a commercial teleport. This converged solution enables voice, data and video traffic over a single IP network to increase efficiency and flexibility, compared with more fragmented, traditional satellite communication networks. Customers benefit from increased bandwidth availability, reduced latency, optimization tools and application flexibility delivered by TCS through an end-to-end Cisco secure IP network.

Handheld Computers Developed for Dismounted C2

DRS Tactical Systems has released the Scorpion line of handheld computers, developed for dismounted command and control and improved situational awareness for warfighters. The product, which is a result of a broad agency announcement contract for the Joint Battle Command-Platform Handheld System, is a COTS handheld computer running the Android operating system and interfaces with tactical radios for the exchange of information on the battlefield. Features of the Scorpion handhelds include a dual core processor for faster application performance, a high resolution 4-inch multi-touch display that allows users to easily pan and zoom without the use of a function key, and an 8 megapixel camera and FlexCharge, which provides the user the ability to charge the device while interacting with tactical radios.



Air Force Civil Engineer to Transform IT Enterprise

CACI International has been awarded a $78 million contract to provide integration, sustainment and deployment services in support of the Air Force Office of the Civil Engineer's NexGen IT program to replace legacy systems with current technologies. The contract was awarded by the General Services Administration Federal Systems Integration and Management Center under the GSA governmentwide Alliant acquisition vehicle and is for a one-year base period and four option years. The Air Force Office of the Civil Engineer provides leadership, policies, resources and oversight in support of the civil engineer (CE) team, which ensures that all Air Force buildings, structures and utilities are maintained and combat ready. The purpose of the NexGen IT enterprise transformation program is to deliver robust mission-focused capabilities that will improve CE productivity and provide the accurate, real-time data necessary to make important strategic decisions and better manage Air Force resources.

Research Seeks Battlefield Jamming Without Interference

The Defense Advanced Research Projects Agency has awarded Raytheon a $3.8 million contract to allow armed forces to conduct jamming operations with minimal communication and control interference to friendly forces. The High-Power Efficient Rf Digital-to-Analog Converter (HiPERDAC) program seeks to enable tactical platforms, such as maritime craft, ground vehicles, tactical aircraft and UAVs, as well as individual soldiers, to conduct battlefield jamming operations while minimizing frequency interference with friendly forces. By generating signals that are both linear (that is, the ability of a signal to remain within a certain frequency) and efficient, HiPERDAC allows jamming across the frequency spectrum while providing precise gaps for communication frequencies used by friendly forces. Achieving signal linearity and efficiency has traditionally been very difficult, particularly at high power levels.

Alliance Offers Encryption Solutions

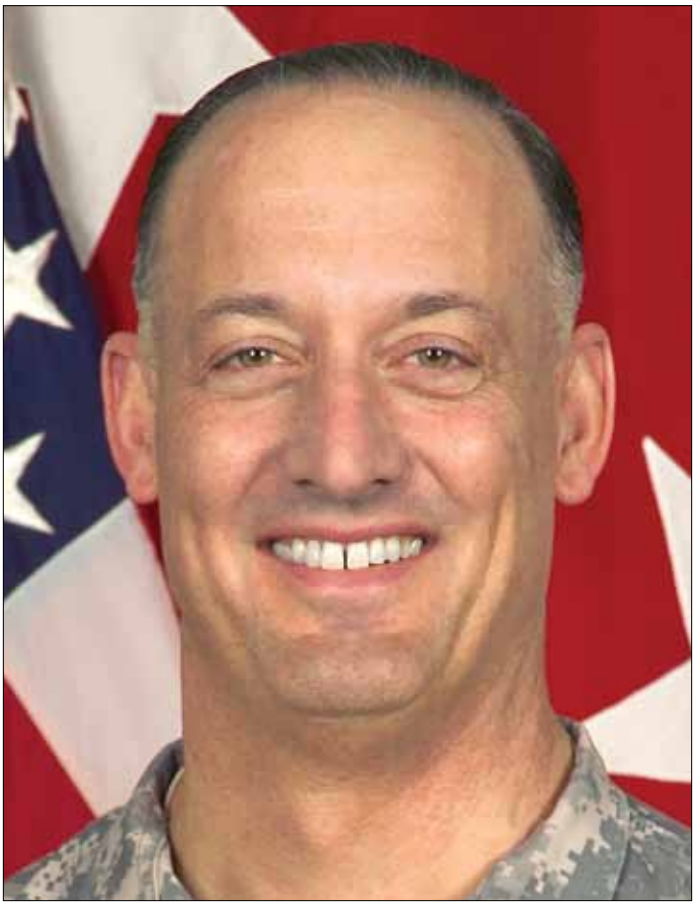
Star Point Corp., a provider of technology solutions and services for government and commercial organizations, and Uponus Technologies, developer of lossless compression and encryption technologies, have formed a strategic alliance. Encryption solutions from Uponus encrypt both streaming voice and data, including video on-the-fly with virtually no latency even in environments where resource utilization is an issue. While resolving the limitations of current technologies that are not able to keep pace with the increasing demands of streaming data, Uponus encryption solutions are easy to use and can be implemented so that they are transparent to the end-user. Uponus' patented encryption technology, called SASE for safe and secure encryption, uses a highly original and non-conventional cryptographic approach which overcomes the limitations of the existing standards. Because of its unique design, SASE is not susceptible to any form of traditional attack or cryptanalysis. SASE encrypted data does not look like encrypted data, as it does not leave any signatures or tells since the output looks like random data or noise.

Signal Transformer

Q&A

Developing Smaller, More Capable Teams and Equipment

Major General Alan Lynn
Commanding General
Army Signal Center of Excellence
Chief of Signal



Major General Alan R. Lynn is the commanding general, Army Signal Center of Excellence (SIGCoE), chief of signal for the Army Signal Corps, and senior mission commander for Fort Gordon, Ga.

Lynn commissioned into the Army in 1979 as an air defense artillery officer. He subsequently branch-transferred to the Signal Corps, serving as training officer for the 5th Signal Command in Worms, Germany. In 1986, he took command of the 324th Signal Company, 72d Signal Battalion, Karlsruhe, Germany, in support of the U.S. Army Europe Main Command Post.

In 1990, he served as the brigade signal officer for the 1st Infantry Brigade, 101st Airborne Division, during operations Desert Shield and Desert Storm. In 1997, Lynn assumed command of the 13th Signal Battalion, 1st Cavalry Division, at Fort Hood, Texas. He deployed the battalion for Operation Joint Forge between 1998 and 1999. While deployed, the battalion supported Task Force Eagle, Multi-Nation Division (North), in Tuzla, Bosnia-Herzegovina.

Lynn was then assigned as an action officer in the Network Management Division of the Joint Chiefs of Staff, J6, at the Pentagon. Following the September 11, 2001, attack on the Pentagon, he was selected as the division chief for the commander-in-chief Operations and Support Division of the J6. He took command of the 3rd Signal Brigade, Fort Hood, Texas, in 2002. In January 2004, he deployed the brigade to 66 locations across Iraq, and was recognized by Congress for creating the largest tactical communications network

In 2005, Lynn was assigned to the Department of the Army Chief Information Officer/G-6 Office as the division chief for LandWarNet Integration Division. He was later selected to serve as the executive officer to the Army CIO/G-6. In 2007, he became chief of staff for the Defense Information Systems Agency, and the following year, he was selected to command the 311th Signal Command (Theater), Fort Shafter, Hawaii.

Lynn graduated from the California University of Pennsylvania in 1979 with a bachelor's degree in English.

Lynn was interviewed by MIT *Editor Harrison Donnelly.*

Q: What is your overall vision for transformation of the Signal Corps?

A: Smaller and more capable: smaller and more capable teams, and smaller and more capable equipment. In one word, µCyber. I envision an iterative yet methodical transformation of the Army communications and IT equipment and systems.

Over the last decade, we moved from a very proprietary communications network, Mobile Subscriber Equipment, to a transport architecture that leverages commercial IP technologies. We have by no means completed this move, since we still have a number of legacy circuit switch based systems out there today, but we have made a lot of progress.

Our next big transition is a calculated leap into the most advanced communications platforms and systems that commercial industry can demonstrate meet a required capability and integrate properly into our existing network and IT structures. I envision these systems as small, lightweight, highly capable and very agile. And I envision smaller, more educated teams of soldiers providing a highly meshed network of points of presence to connect the world's most highly trained, powerfully equipped, uniquely professional warriors that exist today.

Q: What are the chief issues or problems facing the Signal Corps that this transformation is intended to address?

A: Our military has made a massive move from network-enabled to network-dependent; this means that we cannot afford to underestimate the criticality of our Army's Signal Corps. Technology continues to advance, and our adversary has access to more information

and more command and control capability than ever before. This dynamic has the possibility to be the greatest equalizer we have seen in decades.

In order to ensure that our nation never sends one of our sons or daughters into a hostile environment without an overwhelming advantage, we must be able to transform at the speed of technology. Now, this does not mean bleeding edge technology that requires a lot of research and development, but technology that already exists that can be "used as is" or slightly modified for military needs. Most systems today are software defined, making modifications much easier.

Practically, this means addressing the shift in voice versus data, for example. Over the last few generations of technological advances, we have seen a massive shift from communications systems that move voice conversations to one that moves data and full motion video. This is one of the chief issues that we are addressing.

Another issue is the sheer number of communications clusters that must be tethered to our battle command systems, either to pull or to feed information. These clusters require an exponential number of points of presence—many, many more than our current structure provides.

Yet another issue our transformation addresses is the requirement to be able to support the communication needs of either the classic combined arms maneuver scenario as well as the wide area security scenario we have grown so accustomed to over the last decade at war.

Finally, going back to where I started, this transformation of our Army Signal Corps must position us in such a manner that our Army is able to accept and support an iterative-based agile acquisition process that accepts the newest communications systems on a capability set basis.

Q: What are the goals of your micro-cyber initiative?

A: Smaller, lighter and more capable equipment installed, operated, maintained and defended by more educated and thus more capable Signal soldiers. We need to install, operate and maintain a more capable, reliable, flexible, dependable and defendable self-forming, intelligent network that properly stratifies, meshes and delivers overwhelming information dominance.

Sooner is another goal of the µCyber initiative. Since some of the initial advanced equipment we are targeting already exists in joint and special missions units, we are looking at leveraging the testing and lessons learned from these highly trained and highly successful units. If we are going to stay ahead of our adversaries, both in the physical and in the cyberspace domains, we need to capture and integrate game-changing technologies sooner rather than later.

Above all, our soldiers are our greatest strength. µCyber not only includes a shift in education and training, but it requires it. Our soldiers must have the foundational education in the underlying technologies in order to be able to receive iterative changes in hardware that we foresee in the future. The µCyber initiative includes transforming our current military occupational specialty [MOS] producing courses to include a fairly intense three-week common baseline education of basic electronics, communications cable characteristics, and information technology essentials to ensure each signaleer has a thorough understanding of TCP/IP, the OSI model, ports and protocols, computer operating systems, signal flow and propagation, as well as basic information assurance practices and techniques.

I believe that our Signal soldiers are well able to receive this level of education and that this is an investment into each one of them that will pay huge dividends to our Army as a whole.

Q: How will the new Expeditionary Signal Battalions-Enhanced (ESB-E) be organized, and how will they help achieve the goal of providing mission command essential capabilities to the warfighter?

A: The ESB-E of the future will be organized into small teams that have the ability to run multiple systems deployed across a larger area on our battlefields. Unlike today, however, they will be able to provide capabilities to functional and multifunctional brigades and all the way down to the company level. They will be equipped with one large network support package [LNSP] capable of supporting 1,500 subscribers, 17 medium network support packages [MNSP] capable of supporting 200 subscribers, and 51 small network support packages [SNSP] capable of supporting 40 subscribers.

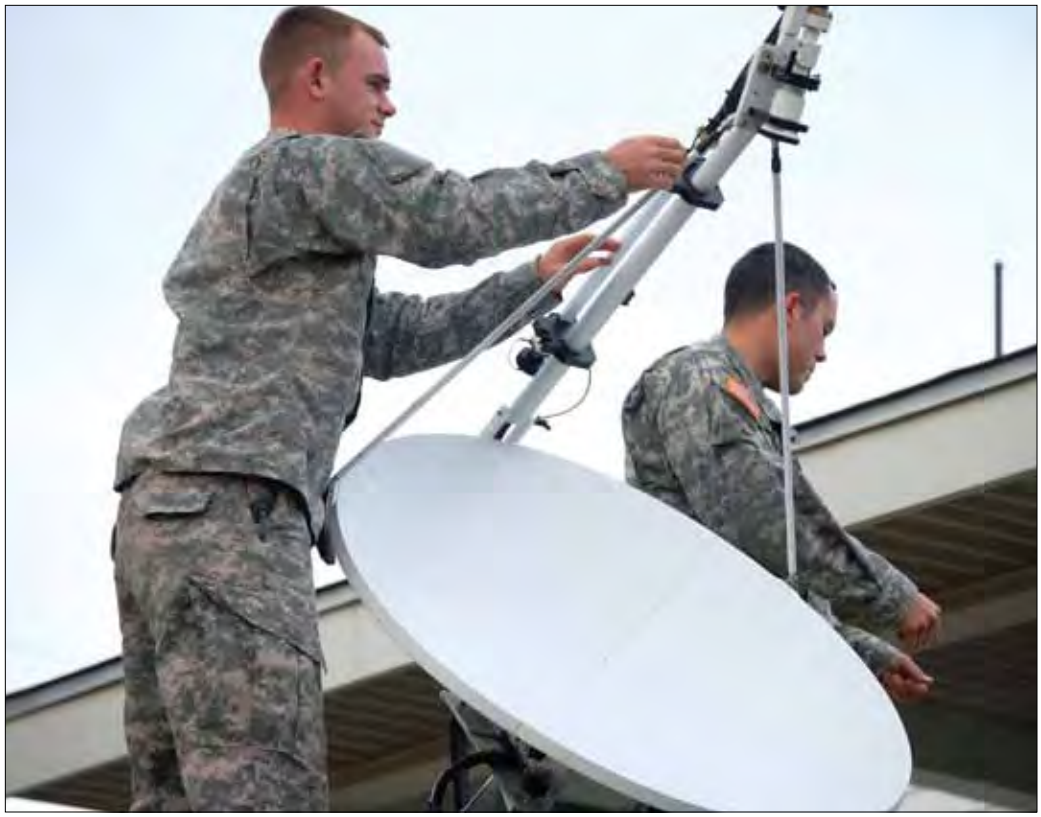
The LNSP is made up of four enclaves focused toward a JTF HQs or a large base camp. The MNSP are stackable, scalable and made up of four enclaves focused on corps, divisions, brigade combat teams, multi-function support brigades, functional brigades and theater level commands. Finally, the SNSP is made up of three enclaves focused toward battalion and company support. Each package has the ability to support any mission assigned by the war fighting commander, including joint, interagency, intergovernmental and multinational, and homeland defense/civil support missions, and can be tailored to support any emerging mission requirement. In short, the future Expeditionary Signal Battalions, the ESB-E, will be more capable and more flexible.

Q: What impact do you see the new mobile communications technologies having on field operations, and how is the Signal Center working to facilitate them?

A: I see opportunities, great opportunities. I also see expectations, great expectations. There are really two separate but related areas that the new mobile communications technologies have brought to light, the first being the smaller and integrated personal communications devices that shift the focus from mostly voice to mostly data with some voice. This is also a generational shift. Many kids today refuse to answer their phone when it rings; they just don't do voice. However, they are simultaneously holding multiple texting conversations and posting and pulling data from Twitter, Facebook, Foursquare, Pinterest and other social networking sites. This is a huge shift in the way we communicate, and the Signal Center is working on integrating communications devices that make this shift to mostly data with some voice into our communications architecture.

The second major area that the new mobile communications technologies have brought to light is mobile applications. The strength in apps is the use of a set of common essential elements that allow developers to create integrated applications that are small and efficient. In the military we tend to create battle command applications as stovepipe systems. Each one comes with its own server and end user equipment, so we add more and more equipment without looking at integration as an ultimate end. Additionally, each battle command application comes with its own standalone essential elements such as maps, position location and timing—all eating up the bandwidth and spectrum that is a precious commodity today. We cannot afford to do business this way anymore.

Say, for instance, that a mobile application developer wants to build an app that will allow you to take pictures during your vacation and store and catalog them in a more graphical way. After you return home you open up a map of the area that you visited. On the map are dots, or thumbtacks; each one represents a picture you took. Each is timestamped, and you merely have to click on the thumbtack and the picture you took opens up. The app developer would not have to create this in a stovepipe. Since your smartphone already has a camera, mapping software, a clock and latitude and longitude information, the developer creates a rather small app that integrates these essential elements in a manner that meets the intent of the app he is developing. This is the direction we need to head.



Soldiers from the 112th Signal Bn., 528th Sustainment Bde., set up a Special Operations Deployment Node-Medium for testing on Fort Bragg, N.C. The Sentinels are USASOC's only organic signal asset, dedicated to providing communications support to SOF personnel deployed worldwide.

We are already developing Army apps and teaching a new cohort on how to build apps. It is the future, much like the Internet was our future. The potential in this realm is limitless. Not only will this result in a much more efficient use of hardware and bandwidth, but we also expect it to change the way we train and use equipment in the future. We expect to purchase equipment in the future that has applications included. These apps will include simulations for educating and training our signaleers on the devices they are issued. Also, I expect these training apps to also be the control application our soldiers will use to configure and operate the equipment of the future.

We believe that this is critical to allow the iterative updates to our communications systems. If we are able to use an app to train our soldiers, and then that same app is switched from training mode to control mode, we will be able to establish and leverage a common set of GUI to sit atop a constant stream of changing hardware. Finally, since these apps can be pulled down, are visual and intuitive and will run in training mode on standalone tablets, units can pull down the new equipment apps months before they are due to get the actual equipment; this means that they will already be familiar, and in many cases already fully trained on these new equipments even before the equipment arrives.

Again, there are great opportunities, but I also see great expectations. There is a perception that we can laterally pull all of this great commercial technology into our signal systems in one fell swoop and that it will be an easy transition. "Well, I can do this at home" is something you often hear.

Unfortunately many of these expectations are actually misunderstandings of the level of complexity needed for ad hoc and mobile networks. We cannot simply pull all of this great commercial technology into our signal systems in one fell swoop. There are configuration, compatibility and security considerations—huge security considerations in fact. When deployed and on the battlefield, the Army must ensure the defendability of networks and systems but we will leverage as much commercial off-the-shelf as practical.

Additionally, the Signal Corps provides the network from the enterprise level to the individual soldier; the complexity of a wireless router purchased for your home cannot even be compared to the complexity of our core routers that must be properly programmed to make millions of routing decisions to include the flexibility to enable mobile ad-hoc network systems such as those within the JTRS program. Also, within your home network, little room is given to prioritization and quality of service [QoS]. QoS and prioritization are very essential when routing and transmitting low priority traffic along with calls-for-fire and a 9 Line MEDEVAC request.

Finally, while we must take into consideration the implications of our current digital generation, which clearly impacts the way they communicate and learn. But it does not automatically mean that these young soldiers understand the theory underlying the digital devices they are operating. It is one thing to set up a Facebook page, and quite another to set up a battle command server.

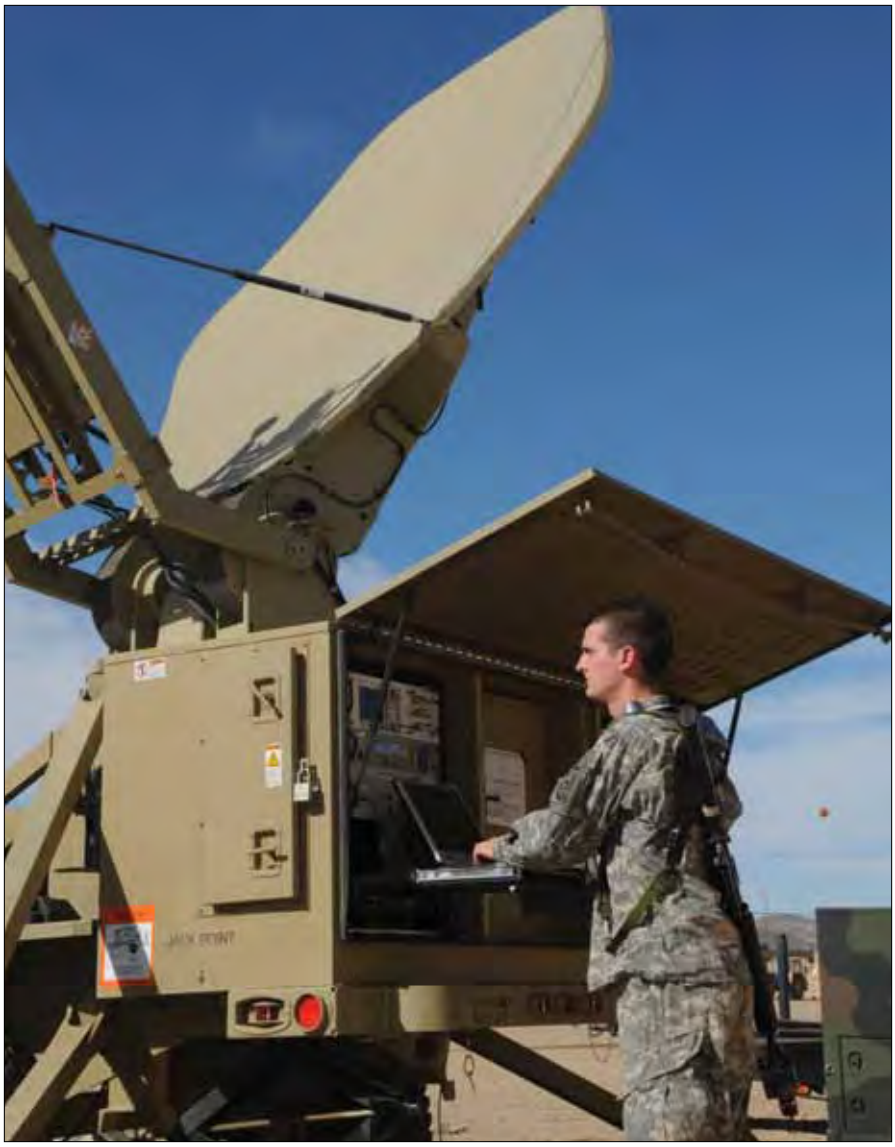
Q: Your recent report on Signal transformation refers to an "antiquated industrial age acquisition system" that is unable to keep pace with modern cyber technologies. What are you doing to change it?

A: Our current system has been entitled a "Cold War" or "Industrial Age" acquisition process. The process is costly, slow and has failed us on many large programs that we expected to provide us the latest technology. As an example, if I offered to go out and buy you the best laptop that money could buy today, but you would have to wait 10 years to get it, would you see that as a good deal? This is

representative of our current acquisition system that was built to deliver tanks and not up-to-date IT equipment.

We are now investing in the Network Integration Evaluation [NIE] at Fort Bliss, Texas, so that we can see what commercial industry can offer us today, test these commercial systems in a military scenario to ensure the systems meet our expectations and integrate with our current architecture, and then invest in newer technologies faster. This is an integral part of the agile acquisition process that allows us to make iterative purchases to get today's technology into the hands of our soldiers as appropriate.

We are also seeking to leverage the Computer Hardware, Enterprise Software and Solutions [CHESS] program to include more signal equipment. Decades ago much of our communications equipment was large, modularized and proprietary. What we are seeing today, however, is a major shift that tells us that many if not most of tomorrow's communications equipment will be common computing devices that act as routers, modems and various other devices. We think now is the time to begin to look at including many of these devices in the CHESS program to allow units that have additional funds to purchase upgraded equipment off of an approved products list.



A soldier works with a (WIN-T) Increment One Satellite Transportable Terminal (STT) during a WIN-T Increment Two Engineering Field Test at Fort Huachuca, Ariz.

Q: How will the ongoing deployment of WIN-T and JTRS affect Signal operations? What significance do you see in the recent decision to drop the JTRS Ground Mobile Radio (GMR) program and move to a COTS-based acquisition for vehicle communications?

A: Our decreasing budgets will bring a quick halt to the days of R&D without quick wins in communications. Trying to fit IT purchasing into the nominative Joint Capabilities Integration and Development System process has just not worked. We either tend to way underestimate what technology will do for us in the future, or to way overestimate it; the JTRS GMR program is an example of the latter.

While JTRS GMR was being developed, commercial industry continued to make iterative updates to the communications devices marketed to the average civilian consumer. Large quantity buys of small relatively inexpensive devices were more than adequate to fuel commercial R&D. Industry was placing more and more sophisticated devices into the hands of their consumers. We found that many of these type of devices may also meet our needs.

The WIN-T and JTRS programs are important. They are the programs of record [PoR] and the methodology the Department of Defense uses to forecast and budget funding. However, where it makes sense we must note where the commercial markets have passed us and use a formalized yet agile acquisition process to bring these new technologies into our PoRs.

In the end, we are working in parallel paths with our commercial counterparts. It makes great business sense to adopt their systems and partner now more than ever before. They have a lot of the same challenges and yet bring a wealth of experience and capability. I believe our budget constraints will drive a lot of the "we" and "they" into "how can we partner?"

Q: Why do you think a reorganization of Military Occupational Specialties is needed? How will that affect both operational capabilities and individual career paths?

A: Smaller, lighter, more agile teams require collapsing skill sets into fewer MOS. We can ill afford "one trick ponies" that specialize in a given system as we have in the past. Systems are becoming more intuitive and our younger soldiers grew up digital, so they get it! In order to bring capabilities down to a lower echelon in our Army we must have multi-capable Signal soldiers that can work multiple systems.

It's basically a math problem. Since we are now required to push capabilities further down into our formations without personnel growth, we have to become more efficient—and with the quality of the soldiers we have today, we can do it. In fact, in many combat locations around the globe our soldiers have already adapted to this new construct through necessity. Fewer MOSs result in smaller, more

capable teams, which gives us the additional numbers we need to make these additional missions possible.

From a career path perspective, we are being careful not to merely combine MOSs, but rather we are taking a clean look at related skill sets that can be better grouped to form stronger technical understanding and thus more capability. In the end, this will also give us an opportunity to do a bottom up review of all enlisted Signal positions and ensure each new MOS has the greatest potential for advancement. Finally, MOS with more skill sets require better educated soldiers; this will be influenced by a new education vice the old training methodology.

Q: What changes are needed in training in order to accommodate transformation?

A: We have to walk away from teaching specific equipment and start focusing on teaching the theory behind them so that as the equipment changes more often and is updated, the soldiers can keep up with the changes—theory remains the constant. We will shift the percentage of education and training much more in favor of education. This is nothing new. If you did a review over the last few decades you would notice it has moved back and forth several times. What we are facing today requires yet another shift.

Technology is advancing at breakneck speeds and as we embrace this through iterative updates within the agile acquisition process, our Signal soldiers must be prepared to receive new equipment more often. To be successful, they must be better educated on the underlying technologies at work within the "boxes" they receive.

So instead of teaching one soldier what knobs to turn and what buttons to push to turn on and operate a line-of-sight microwave system, and another soldier a tropospheric scatter system, and a third soldier a satellite system, we will teach these three soldiers radio wave propagation theory, so they each understand why two are line-of-sight waveforms while the other bounces off the troposphere. After this education, any of these soldiers will have the ability to turn on and operate any one of these systems, and when the systems are collocated, we only need one of them, not two or all three.

Another area that will help us is lifelong learning. One technique to institutionally provide resources to gaining units is to move as much training as possible to the virtual environment—in other words, training apps. If each system is fielded with both simulation software, so soldiers could virtually walk around and manipulate the equipment, as well as an application that can run on a smart-pad or similar device that allows various scenarios to be encountered, including various startup configurations and a number of fault location and correction exercises, our operational units would benefit greatly.

Since the Army cannot afford to do a pure-fleet update of equipment, a unit further down the fielding plan could download the training app well in advance of their receipt of the equipment and thus be already trained and proficient prior to the actual equipment hitting their property book. And better yet, if the training app could be switched to operate mode and then connected to the equipment through an authentication process, soldiers would only need to learn one application.

Q: What can industry do different or better to support Signal transformation?

A: Basically, we are looking for four things. But before I address them, I would like to take this opportunity to thank our many commercial industry partners for their sacrifices and hard work during this last decade of war. Not many Americans have a true understanding of what our armed forces have endured during this protracted period of intense conflict, nor how many companies have stood by our side sending many representatives to combat zones. To all of them I say, thank you.

Now, the first thing I would ask industry to do different is to use technology to make the install-operate-and-maintain part of our mission simpler. We might never get to the point where setting up a router in our LandWarNet is as easy as pulling a NetGear 802.11n wireless router from the bag and running up your home network, but we must make technology interfaces simpler and intuitive. We are pushing more and more capability to the edge, down to the lowest echelon, where our most junior and inexperienced Signal soldiers fight. We must make these devices easy to set up and turn on for operations, and if they need complex configurations to properly enter the network, we must make them in such a way that they lend themselves to initially enter into the network in a "do-no-harm configuration mode" to allow remote configuration by an echelon where the appropriate level of skill exists.

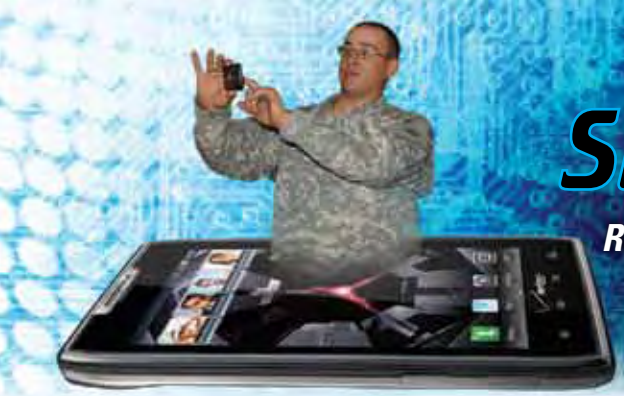
The second thing I would ask industry to do differently is to stop using proprietary code and equipment when commercial standards will work. We understand that our many commercial industry partners must watch out for profits and the bottom line. With the vision of iterative changes every few years, however, the field is going to be open for many to make a profit. Actually, if a vendor uses such proprietary techniques, they may push themselves right out of the competition. In the end, industry will make more profits by not using proprietary code and devices. Going the extra mile to make COTS systems will just make them late to market. Also, by using open standards and commercially available equipment modules, the commercial market has the ability to open up its wares to a much broader community of buyers.

The next thing I would solicit industry to do is to bring their best products, with commercial standard protocols, to the NIE. I know that many are waiting to see if the Army will end up making an acquisition decision at the conclusion of an NIE event; let me assure you that we will. The key word of Network Integration Evaluation is integration. And the best way to ensure integration is through the use of open commercial standards and protocols. I know that we are asking commercial industry to make an investment, but isn't that what open competition is all about?

Finally, I ask industry to embrace our new education and training strategy by including training apps as part of the overall equipment packaging they put together for the Army. Since we are looking at including this as a requirement in the future, it only makes sense to work these apps codes together as part of the overall programming effort. In the end, we want these training apps to also be the GUI interfaces that will actually operate the systems. They should be visual and intuitive like today's smartphones.

Q: Is there anything else you would like to add?

A: Yes: It is a great time to be in the Signal Corps, and the future looks even brighter as we develop both our signal and cyber skills. Thanks. ✯



Smart and Rugged

Ruggedized options for smartphones increase as military use grows.

By William Murray
MIT Correspondent

With the increased use of smartphones in the Department of Defense, it was only a matter of time before vendors began offering ruggedized versions. Purchasers of these devices are finding that ruggedization doesn't necessarily entail great expense because the device manufacturers and wireless carriers are able to sell the units across several industries with demanding requirements for use, enabling them to tap into a broader market.

While no standard definition recognized across industry exists for smartphones, they generally feature the ability to make and receive telephone calls, edit word processing and spreadsheet documents, maintain calendars, surf the Web, download smartphone applications and send and receive emails. So the smartphone clearly represents a hybrid between a microcomputer and a mobile phone.

The mobility of the device, its ease of use and its computing power represent three primary benefits of using a smartphone, but a smartphone's mobility increases the potential damage that the device can incur. The average life cycle of a smartphone is two years, which reflects in part the damage that many units receive because of their heavy use and mobility. Using such devices also allows the military to access 3G and 4G networks without being saddled with the expenses of developing and operating such global voice, video and data networks.

In addition to fulfilling the military's operational needs for smartphones and cell phones that can meet military specifications for shock and vibration and water and dust intrusions, vendors are also offering mobility management, so that military users can better secure their networks and the smartphone devices when units get lost or stolen.

In December 2010, Sprint made one of the first forays into the ruggedized smartphone market, announcing the Sanyo Taho, built to military 810G specs to withstand dust, shock, vibration, extreme temperatures, blowing rain and immersion, and priced at less than $100. The Sanyo Taho by Kyocera also features a clamshell form factor, a 2-megapixel camera with LED flash and video capture support, GPS, Bluetooth connectivity and microSDHC support. Sanyo Taho's ergonomic shape is covered in a non-slip Dura-Grip texture to ensure a solid grip.

Verizon Wireless sells the Casio G'zOne series to the military, which meets the MIL-STD-810G requirements for immersion in 1 meter of water for 30 minutes, a one-hour vibration test, heavy dust for six hours and a drop at 1.22 meters. Moreover, the Casio G'zOne withstood Department of Defense testing and worked after being exposed to saltwater spray for 24 hours and 95 percent humidity for 24 hours. It has withstood MIL-STD-810G certification testing for high temperature up to 85 Celsius for 96 hours and -25 Celsius for 96 hours, according to company officials.

Danny Johnson

Motorola Solutions provides ruggedization on its mobile computing devices, such as the MC3090-Z and the MC75A and the ES 400 smartphone, according to Chris Ventura, vice president of U.S. federal government solutions for the company. Ruggedization includes shock and vibration and water and dust intrusion. In addition to the military, transportation and logistics companies, warehouses and manufacturing facilities have a need for ruggedization features, Ventura noted.

In addition to DoD adoption, Casio officials are seeing their ruggedized smartphones purchased by construction, landscape, law enforcement and Transportation Security Agency users. It is important that wireless providers and equipment manufacturers find additional markets for ruggedized smartphones, since having a broader market enables them to sell more devices and encourages innovation and helps them to achieve economies of scale, which over time brings down the costs of the devices.

Mobility Management

Mobility management is a key feature that DoD officials are seeking, noted Danny Johnson, Verizon Enterprise Solutions' director for public sector vertical solutions. Mobility management has to do with the CDMA and GSM networks and their ability to identify and track cell phone devices on their networks.

"There's a growing need to manage these devices," Johnson said. "How do I manage these devices in total on a network? The old paradigm was, information technology was locked down and computers were issued centrally." With handhelds, by contrast, users can bring them to the enterprise from previous assignments or from their own use.

DoD has a strong need to "wipe clean" mobile devices that get lost or stolen, so that any sensitive or secure data is removed from the devices, added Johnson, whose company offers a total of 21 ruggedized smartphones.

"There are two issues: policy and the device itself, and how we can best secure it," Johnson said. "There are overlapping requirements in security and policy." Policy on smartphones and personal digital assistants can come out of the military services as well as the Office of the Secretary of Defense in 2012 and beyond, according to Johnson.

Johnson noted that the increased acceptance of smartphones and interest in ruggedized smartphones in DoD coincides with the "sunsetting" or retiring of proprietary military networks that would have allowed previous generations of mobile devices to operate in a secure environment. He said he is encouraged by the increased adoption of smartphones in the military and sees the challenges as part of the broader difficulties brought about by the "consumerization of information technology," meaning that easy-to-use and ubiquitous devices such as smartphones that are used by consumers eventually make their way to enterprise IT networks created by the military and other organizations.

Casio, Motorola and Verizon Wireless officials were tight-lipped about the potential market size for ruggedized smartphones in

DoD, but they clearly seem clearly optimistic, even though the devices are usually sold through limited channels during this early stage of adoption.

"We are expecting increased adoption of our smartphones in the U.S. military, now that the AME 1000 is available for shipment," Ventura said, referring to Motorola Solutions' AME 1000 Secure Mobile Telephony Solution, which combines hardware-based cryptography and certificate management with a software-based secure voice application on an ES400 smartphone.

The AME 1000's Motorola CRYPTR micro combines hardware-based encryption and key management in a microSD form factor that supports both Federal Information Processing Standard (FIPS) 140-2 Level 3 and Full NSA Suite B Cipher Suites, according to Motorola.

"The Army's medical community uses our rugged mobile computing devices to track patients from the battlefield to the hospital," Ventura said. "And we see a significant opportunity within DoD for the rugged smartphone, especially when the high-level security features of the Assured Mobile Environment (AME) are considered." He said that ruggedization features are a nominal cost above the price for commercially available smartphones, and that the cost depends on the device and application.

The Motorola AME 1000 has secure voice capability through Apriva Voice, an NSA Suite B Voice over Internet Protocol (VoIP) application for AME 1000 users. It can operate around the world, since the Motorola AME 1000 can work on both of the two dominant networks, CDMA and GSM. The Motorola AME 1000 also features forward and backward compatibility to legacy secure infrastructure and existing secure mobile devices and future Secure Real-time Transport Protocol-Datagram Transport Layer Security commercial standards, which use Apriva's VoIP technology.

The Motorola AME 1000 has the ability to enable users to run two operating systems, with one running trusted applications and the other untrusted applications, according to Gary Schluckbier, director of engineering at Motorola Solutions Secure Products Group.

Android Models

Three ruggedized Android smartphones are the Motorola DEFY+, the Samsung Galaxy Xcover and the Sony Ericsson Xperia Active, which run the Android 2.3 operating system. They feature 512MB of RAM and at least 3-inch displays. The DEFY+ has 2GB internal storage.

Johnson called Verizon Wireless' Droid Razr smartphone, with its embedded security features and ruggedization, a "military-designed phone."

The Android operating system would seem to have a ruggedization advantage over its biggest competitor in the military market, the Apple iPhone, because Android is much easier for third parties to customize. Apple has made its products primarily for the consumer market, and analysts say it is less apt to allow third party development, particularly in light of its spectacular success in the consumer market and in terms of stock valuation.

Despite Apple's evident lack of interest, however, there is good news: iPhone users can purchase cases for their devices that increase their durability substantially.

"From a technology perspective, it's doable," Verizon Wireless' Johnson said of the iPhone being ruggedized for military and other vertical market usage. "Does Apple want to make the investment?"

Quite a few ruggedized phones are flip phones, such as the Samsung Convoy 2, which Verizon Wireless offers.

Sprint plans to offer Kyocera's DuraPlus unit, with a sturdy front-ported speakerphone for noisy environments, during the first half of 2012.

Early this year, Sprint announced the Kyocera DuraPlus, one of the first phones to work with Sprint's new Direct Connect push-to-talk service, launched in the fourth quarter of 2011 to work with Kyocera and Motorola's rugged devices. The DuraPlus conforms to Mil Spec 810G, so it can withstand shock, vibration, temperature extremes and blowing rain. The DuraPlus can give users as much as 9.5 hours of battery life.

In addition, the unit can survive immersion in 1 meter of water for as long as 30 minutes. The DuraPlus also features an embedded LED flashlight with a separate power button to help users during power outages and nocturnal operations.

Security Issues

Mike Ligas, DoD sales manager for Sprint, noted that the increased adoption of smartphones enables the military to make its personnel more productive because they can work on the go. He noted that wireless carriers such as Sprint can implement extra security on the wireless interfaces that customers use through a Type 1 security device, which can diminish the danger of data or voice calls being intercepted or any information falling into the wrong hands.

Because of their concern for smartphones being hacked into and video or audio being intercepted from meetings, some military and intelligence community users of smartphones not only turn their phones off during meetings, but also remove the devices' batteries to ensure that they cannot be operated remotely through a wireless network.

Mark Bigham, vice president of business development with Raytheon Intelligence and Information Systems in Garland, Texas, sounded a note of caution about ruggedization of smartphones in DoD. "As soon as you start going with a custom phone, the price goes up exponentially and creativity also starts going down.

"A militarized version of commercial phones is where smartphone work needs to go," Bigham said, noting the importance of the FIPS 140.2 standard, which NIST and the federal government first unveiled in 2001 as a means to accredit cryptographic modules.

"FIPS 140.2 is becoming more relevant" with smartphones and their use on DoD enterprise networks, Verizon Wireless' Johnson said. Data at rest encryption is very important, as are Virtual Private Networks encryption standards that FIPS 140.2 covers.

Raytheon has developed the Raytheon Android Tactical System, a combat-ready Android application, which allows users to place members of their combat team as well as objects such as planes on their buddy list, and track them using GPS.

Verizon Enterprise Solutions, meanwhile, is playing an important role, since the company purchased a 400 MHz block of 4G spectrum through a Federal Communications Commission auction. Through FCC regulations, Verizon Enterprise Solutions has created an open access network so that handset manufacturers such as Casio, Honeywell, LG Electronics and Panasonic can certify their platforms for use on the 4G network. ✯

For more information, contact *MIT* Editor Harrison Donnelly at harrisond@kmimediagroup.com or search our online archives for related stories at www.mit-kmi.com.

ID Management's New Challenges

GOVERNMENT AND INDUSTRY TACKLE ISSUES SUCH AS THE SECURITY OF REMOTE AND MOBILE NETWORK ACCESS.

BY PETER BUXBAUM
MIT CORRESPONDENT

After a number of years spent working out the technology and procedures, the process for establishing the identifies of individuals who are allowed access to military networks has largely been settled, at least for now. But new needs and capabilities are shaking the world of identity management, particularly as the popularity of mobile computing grows.

The 2004 Homeland Security Presidential Directive 12 (HSPD-12) required federal agencies to issue a federal personal identity verification (PIV) smart card credential for access to federal information systems. Within the Department of Defense, that requirement was met with the use of the Common Access Card (CAC). Ninety-seven percent of DoD employees and authorized contractors have now been issued those cards.

Establishing the identity of authorized individuals takes place on the basis of two-factor authentication: "Something you have"—the CAC—and "something you know"—the cardholder's PIN code.

There is still some work to be done on the basics. For one thing, many military agencies and installations have implemented their own home-grown access systems, not all of which are HSPD-12 compliant.

Beyond that, many military agencies, and the vendors that support them, have moved on to other and more complicated issues. They are tackling the issue of the security of remote and mobile network access. They are creating systems that broaden the notion of identity management to include the provisioning of all credentials and materials necessary for personnel to perform their missions through access to the equivalent of an app store.

Lisa Kimball

lisa.kimball@telos.com

Nelson Cicchitto

nelsonc@avatier.com

Industry is building data storage systems to ensure the security and reliability of identity data, and is pondering the possibilities of collaborative credentialing, which would facilitate the acceptance of identities across different organizations and networks.

"The identity and access management industry as we know it is evolving into a commodity," said Nelson Cicchitto, chief executive officer of Avatier. "The core technology challenges have been solved. It depends how much time and money your organization is willing to spend on getting it installed, as well as how much it will cost to keep it running [once it has been deployed]. It's basically broken down to a series of application programming interfaces. The industry is moving on to other areas."

"DoD has a well-established process for proofing identities and providing access," said Lisa Kimball, vice president for Defense Manpower Data Center (DMDC) operations, Telos Identity Management Solutions. Telos ID works with the DMDC to supply and integrate the hardware that is used to vet the backgrounds of individuals applying for CACs.

There are still challenges associated with the provisioning of personnel with access to network resources. "Getting identities established is the first step," said Yves Massard, director of product line management at ActivIdentity. "Once we know who a person is, we can provision that identity with access privileges. The issue of who gets access to what is done at the agency or service level is probably better determined locally. It is also necessary to update identities as people leave organizations and switch jobs."

Some military agencies are still updating their systems to comply with the requirements of HSPD-12. "HSPD-12 requires that identity management rely on public key infrastructure (PKI) systems," said Massard. "Many applications that have been procured or that have been developed in house in the last 10 to 15 years don't incorporate those concepts and can be difficult to update."

A PKI enables users of a public network such as the Internet to securely exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Yves Massard

Remote Access

Another area that industry is working on involves remote access to networks. Laptops and BlackBerrys can gain remote access to military networks, and the list of platforms and operating systems in that category will be growing in the near future.

Security is still an issue with remote access for some. "Remote access is easy," said Tony Busseri, chief executive officer of Route 1. "The challenge is ensuring security that protects your organization's sensitive data and prevents network and employee information from being compromised, especially when data is accessed from outside of your organization's network."

Allowing access to network resources across organizational lines, for example, among military and intelligence agencies, would be useful in facilitating collaboration and enhancing security, according to Kimball. "It's all about trust," she said. "You need access management and policies that are accepted across organizations. You need agreement about the verification processes. Collaborative credentialing is all about enabling logical access down to the individual file level if necessary."

ActivIdentity provides solutions for identity and access management. The company's credential management solution has been used by DoD and other federal government agencies to issue credentials such as PIVs and CACs.

A solution called 4Tress allows organizations to upgrade their authentication systems to become PKI compliant. "4Tress can adapt to different authentication methods including PKI and smart cards and it's also capable of integrating with those applications," said Massard. "For example, if an organization is using only a user name and password, by hooking up with 4Tress, it can be used as an application portal to become PKI enabled. You don't need to write any lines of code or do any integration."

ActivIdentity's other solutions can be used to assert the validity of identities in real time. "It is linked to PKI and can determine whether a smart card is valid at the time of a transaction, also in real time," said Massard. "We also have a mobile application that can validate identities remotely when a smart card is inserted into a handheld device."

ActivIdentity's solutions have been installed throughout DoD. "Our system has been used to issue every CAC card issued by DoD," said Massard. "So far there have been more than 25 million CAC cards issued."

Route 1 offers a system that differs from how authentications and access management is typically done today. Remote access to networks is usually accomplished through a portal. As part of the process, data is pulled from behind the enterprise firewall to the local device in order to complete the authentication. Route 1's system, by contrast, has the authentication process taking place within the organization's network.

"We are huge believers in one fundamental thing: Data should never leave the network," said Busseri. "When access is done on a virtual private network, data is extracted from the enterprise network and pulled from behind the firewall to the remote computer. That is not right for security."

Route 1's system emulates the architecture of a traditional mainframe computer that makes use of "dumb" terminals. That means that the terminals can display data, but the data remains within the mainframe. No data is pulled from the mainframe to the terminal, which possesses no computational abilities.

In the case of Route 1's identity management system, the authentication data remains behind the origination's firewall in a secure cloud. The user input is transmitted to the cloud, where the authentication if performed. At no time does the data breach the enterprise firewall.

In a solution that Route 1 provided the Navy, the company incorporated a CAC swipe for access from remote and mobile devices. "Why would you use any different authentication process for digital remote access?" said Busseri. "The biggest security risk to networks today is not doing a good enough job for mobile computing. We use the same multi-factor authentication process that the military uses for internal network access. The sign on for a computer sitting inside the fortress is replicated externally."

Web Service Platform

The Avatier Identity Management Suite (AIMS) is one of the first identity foundations to employ a familiar IT "shopping cart" experience to place access accountability in the hands of the reporting structure and military hierarchy. According to Cicchitto, "This foundation automates daily operational processes, such as user provisioning, user requests for resources, group management, access certification, enterprise password management and risk management."

"These days, IT organizations are faced with more projects than they have staff or time to implement," said Cicchitto. "With typical identity management systems for a sizable organization, you need dozens of people to manage the environment, develop new features and capabilities and man the help desk. We don't believe you should need such a team for 100,000 users or even for a million users. Avatier takes a new innovative approach to achieve rapid time to value with the lowest operational cost in the industry."

Avatier is pursuing an approach that it called "access management by request."

"A person's identity within an organization includes everything he or she needs to do the job from access to network resources to obtaining physical assets such as laptops, mobile devices and controlled facility access badges and keys," Cicchitto explained. "All those resources become part of your identity and make up who you are. Then, when you leave the armed forces, these items need to be recovered and accounted for, and the slate wiped clean. The only way to manage this is through a robust request system that offers flexible automated approval workflows."

"AIMS can be deployed in small environments in a single day with little to no client-side programming," he said. "A key differentiator

for Avatier is time to value and operational efficiency. Tools have become so complex that you have to rely on big consulting firms and spend considerable time, money and internal, already constrained, resources to get them implemented and configured. We have simplified identity management to the point where business owners can easily manage the identity store interface without programming or development."

The system also simplifies provisioning requests for the user. "If you can shop for apps in an app store or shop on Amazon," said Cicchitto, "you should be able to browse, request and receive access, whether that includes enterprise applications, home-grown applications, cloud applications or physical assets like laptops, mobile devices, controlled badges or facility access keys. All of these things can be incorporated into an ITIL supported business services catalog that can be requested and accessed through something similar to an online app store."

All the workflows are built into the store, and request workflows are constructed automatically. "The workflows consist primarily of the approvals required to validate user requests based on rules built into the business services catalog," said Cicchitto. "That is our vision of where the future is headed."

Avatier's technology is also platform independent. "It is independent of the mobile device or the browser on the desktop and the advantage is that it simply works for everyone," said Cicchitto. "There are no clients for individual platforms to write to Windows, Mac or Android."

Avatier's environment is also very secure. "It went through multiple third-party source code and vulnerability scans along with penetration and SQL injection tests—resulting in more than 600,000 unique tests across several calendar days," said Cicchitto. "As a result, Avatier's entire Identity Management Suite has been added to the Air Force evaluated and approved products list due to representing minimal risk to the Air Force Global Information Grid."

Avatier is implementing its AIMS Identity Enforcer solution within the Air Force, where more than a million identities will eventually be centrally managed with the system. "We are looking forward to putting this in the ring and showing what we have done for government agencies and what we can do for DoD," said Cicchitto. "We will be submitting a concept for a governmentwide identity management foundation."

Avatier's pre-integrated solution, on average, provides customers with measurable return on investment in less than a year, according to Cicchitto. "Avatier's customers also benefit from their investment with more productive employees and enhanced security," he added. "The big advantage is that you get what you need without involving your help desk. Organizations can be focused on tasks that are important. Access requests will not impact the time and money the armed forces and their IT staffs could otherwise spend on new technologies that further their individual and vital missions."

Hardware Issue

There is a potential hardware issue to identity management as well. "Identity data may be kept and retained for long periods of time," said Patrick Humm, president of Hie Electronics. "A lot of this data has a lifetime longer than the lifetime of some of the equipment it is stored on. For example, a typical hard disk drive data will last four years. Then you have to replace the hardware and migrate all of the data. Whenever you do that, there is the potential for the loss of data."

Hie Electronics provides a data storage platform called TeraStack, based on Blu-ray optical media that has been independently tested to a 50-year life without data loss. "Disk drives and tape do not have that attribute," said Humm. "They do lose data over time."

TeraStack provides 92 terabytes of storage, but that number is growing as the capacity of Blu-rays increase. "As the density goes up, we will be going to 132 terabytes next year," said Humm, "and in 2014 we will see a step function to 500 terabytes on a single system. This requires less data migration and replacement of hardware and reduces the risk that you will lose some percentage of your data."

Identity management should be moving toward "collaborative credentialing," under which military branches and agencies and their contractors could access appropriate portions of each other's networks. The same situation might come about between DoD and intelligence community.

The national security community is the ideal place to champion that sort of process, according to Kimball. "The CAC would need to receive even greater acceptance," she said. "It is already the gold standard for cyber-identity. DoD has a vetting and proofing program. No one gets a CAC until a background investigation, and the DMDC gets the green light from an FBI print check."

At the process level, collaborative credentialing involves creating an atmosphere of trust among organizations. "The CAC should enable organizations to have trust in each other," said Kimball. "DoD and the intelligence community need some agreed standardization on the use of CAC for logical access so that one organization doesn't have a lower level of security than the others."

But it is not as simple as just that. "It comes down to trust and it comes down to personalities," said Kimball. "To a great degree you need trust between organizations so that the credential can be accepted across organizational lines.

"Management resistance is an enormous challenge," she added. "It seems that department officials prefer to do their own background vetting. Perhaps that is because this vetting has become a cottage industry."

As local offices and installation implement their own access systems, including using their own credential with its own rules and regulations, managers and commanders may want to use their own contractors to do the vetting.

Future identity and access management systems will likely be more readily accessible remotely and will require higher levels of security. Massard foresees that they will be available on more and more types of mobile and handheld devices.

"It is already readily available on laptops and BlackBerrys," he said. "We are looking to extend those products to other mobile platforms. As policies change and different types of mobile devices gain acceptance within the military, we want to make sure that identities can be managed securely on whatever device is being used."

Busseri projects that the military will be adopting third-factor authentication of identities for logical access in the form of biometric characteristics. "Three factors of authentication is where the market will move," he said. "We expect military organizations to be adopting that paradigm." ✯

For more information, contact *MIT* Editor Harrison Donnelly at harrisond@kmimediagroup.com or search our online archives for related stories at www.mit-kmi.com.

Compiled by KMI Media Group staff

System Connects Warfighters to the Tactical Cloud

Harris has unveiled the Harris Falcon networking system, the first end-to-end system for connecting warfighters in the field to the tactical cloud. The system broadens and simplifies the delivery of secure video, data and other crucial command and control applications over both wideband tactical and emerging cellular networks. The new system combines information technology resources, such as a computer server and Falcon wideband tactical radio, into an integrated, lightweight package that can be deployed to support missions at the tactical edge. By utilizing the Falcon networking system, tactical users can now access applications and other critical data files that were previously beyond their reach due to constraints in bandwidth and power. To help transform the user experience in military communications, Harris designed the Falcon networking system with a 4G tactical cellular module that will enable warfighters to use ruggedized smartphones and other lightweight devices on the battlefield. Harris also has introduced a ruggedized tablet device for military applications that is designed to integrate with the Falcon networking system. The latest Harris integrated networking system includes Falcon III multiband tactical radios, a network communications server, tactical cellular transceiver and intuitive edge devices. Built for upgradeability, the system can expand to incorporate additional devices.

Mobile Ops Center Based on Intelligence Security Standards

MTN Government Services has announced the immediate availability of its new Re-Deployable Secure Operations Center (RSOC), the industry's most secure, self-standing mobile facility. The RSOC is a solution that can be drop-shipped into any environment and assembled within days by only a couple of installers. The structure is self-supporting and is capable of withstanding multiple disassemblies and redeployments without degradation. This enables both government and commercial organizations, including military operations, oil and gas, construction and data centers, to invest in a secure mobile facility that delivers long-term return-on-investment. The RSOC's construction is based off of the Intelligence Community Directive 705, the highest possible security standard used by the U.S. government. The facility is constructed of 4-inch thick modular panels, welded with inner and outer steel with high-density insulation to aid in exceeding sound attenuation standards. In addition, there is a unique sound masking device and RF Shielding. Power, data and voice connections pass securely through a customizable enclosure to fit all needs for CONUS, OCONUS and MIL-Spec connections.

Durable Connectors Used for Military Communications

ITT Interconnect Solutions has developed a custom, highly durable and low-cost MIL-DTL 38999 Series II connector that features a contact for a printed circuit board and a rear seal for use in corrosive environments. Constructed to customer specifications, the interconnect solution was not only designed to be intermateable with standard MIL-DTL 38999 connectors, but also to withstand thermal cycling and exhibit air pressure sealing to a mandatory 5 PSI. ITT engineers created the MIL-DTL 38999 Series II connector as a modification of an existing product, thus reducing the cost of custom tooling for the customer. Applications for the low-cost hermetic custom MIL-DTL 38999 connector with printed circuit board contact include military communications systems, such as portable radios and military vehicle radios.

Mobile Satellite Solutions to Provide Disaster Backup Services

As the storm season begins, Verizon will be offering general availability of its Mobile Satellite Solutions to provide dependable backup services and enhanced disaster recovery when normal communications are disrupted.

Building on its extensive experience providing satellite services, Verizon has enhanced its Mobile Satellite Solutions suite, originally announced last August, with an environmentally controlled inflatable shelter that joins other service equipment such as auto deploy kits, communications trailers and an executive coach vehicle. These 20-by-20-foot air shelters provide a complete communications solution incorporating Verizon satellite, wireless and IP data networks. With a rapid setup of less than 20 minutes, the air shelter has ample workspace with solid doors, a floor, windows and integrated LED lighting to provide a safe, comfortable work area for up to 12 adults, while protecting them from severe weather conditions.

In addition to the numerous equipment configurations available, Mobile Satellite Solutions includes experienced planning and integration assistance to reduce the risk of interruptions that can impact communications. Beyond business continuity, customers looking for primary access, digital signage, IPTV or content delivery will find that Verizon's Mobile Satellite Solutions allows them to take advantage of the powerful combination of advanced satellite technology and Verizon's global IP network.

Advertisers Index

Calendar

April 16-18, 2012
Sea Air Space 2012
National Harbor, Md.
www.seaairspace.org

April 16-19, 2012
National Space Symposium
Colorado Springs, Colo.
www.nationalspacesymposium.org

May 7-10, 2012
DISA Mission Partner Conference
Tampa, Fla.
www.disa.mil

May 15-17, 2012
Joint Warfighting
Virginia Beach, Va.
www.afcea.org

May 15-17, 2012
GSA Training Conference and Expo
San Antonio, Texas
www.expo.gsa.gov

June 4-8, 2012
GEOINT Community Week
Washington, D.C. area
www.usgif.org

July 10-12, 2012
TechNet Land Forces—South
Tampa, Fla.
www.afcea.org

August 14-16, 2012
TechNet Land Forces—East
Baltimore, Md.
www.afcea.org

Thomas Foust
Vice President of Global Network Solutions
Intelsat General Corp.

Q: What do you see as the most important trends in the military market for commercial SATCOM?

A: Based on the changing relationship we have with the U.S. government and the growing demand for satellite capacity, we see hosted payloads and ISR, specifically UAVs, as key trends for the coming years and ones that we will support.

For hosted payloads, we see some very encouraging signs within the government. First, we just launched the UHF hosted payload for the Australian Defence Force (ADF) on IS-22. This will give the Australian military much needed UHF capacity to support tactical communications. This payload will also provide DoD with additional UHF capacity as part of their contract with the ADF. In addition, we see leadership in the U.S. government moving in a positive direction. For instance, the addition of a hosted payload office within the U.S. Space and Missile Systems Center is sending a very clear signal to commercial operators. This needs to be followed by action, but it is clear that hosted payloads are becoming a central part of the dialogue on how to affordably address space missions.

Increased UAV construction and use is a huge growth driver for the satellite communications industry right now. The Secretary of Defense's strategy calls for a 30 percent increase in the U.S. fleet of armed unmanned aircraft. This would include possible surge operations that would require more than 200 MHz in additional capacity. As some DoD officials have recently said, fewer boots on the ground means more eyes in the sky. These eyes in the sky also demand more satellite capacity to support the growing sophistication of on-board sensor suites. Intelsat General looks forward to helping meet this demand based on the current support it gives—over 950 MHz of bandwidth for about 70 UAV missions.

At the same time, civilian use of UAVs is on the rise. And, with the increased

budget pressures on the U.S. federal government, other governments may become more interested in financing their own UAV efforts, which will be good for the market as a whole.

We also see communications on the move as an important opportunity to support our government customer. They have come to depend on their ability to send and receive data from any location, and they need high data rates to do so as effectively as possible. We are looking at many ways to use our fleet of satellites to support this requirement, offering continuous worldwide broadband coverage to maritime and aeronautical customers.

Q: How is Intelsat working to ensure affordable access to space at a time of federal spending cuts?

A: All of us in the government space market are in the vanguard of a challenging new era. Very difficult questions that haven't been relevant for over a decade will now need answers. What programs do we keep? Which do we cut? Are there better, more efficient ways to accomplish a particular mission?

It's understandable but unfortunate that we are at the initial phase of the government's reaction to the new budget culture for space, which we call "hunkering down." Not only does this impulse prevent reaching out for help, but it also becomes such a focus that executing on the mission suffers. Hunkering down also prevents any coordination among branches of the military, hurting chances for a coordinated and strategic response to this country's space challenges, especially the balance of MILCOM vs. COMSATCOM.

There have been some encouraging signs of change. It was a major goal of the 2010 National Space Policy to make more and better use of commercial networks that are already operational, proven and ready for use today. Intelsat General's support for the Navy through the CBSP program is a good example of this approach. Additionally, DoD is sub-leasing UHF capacity on the ADF's hosted payload on board the recently launched Intelsat-22 spacecraft. This hosted payload is saving the ADF over $150 million and cutting years off deployment time. The U.S. government could realize similar benefits by leasing hosted payloads directly from commercial operators, and indications are that they are slowly moving in that direction. Programs like these are why we're optimistic about the future, despite the tough budgetary climate.

Q: What potential do you see for military and intelligence users from hosted payload programs?

A: Hosted payloads offer government customers an expedited method to access space on an economical basis as compared to stand-alone military satellite programs. By hosting a payload on a commercial satellite, customers share launch, insurance and construction costs. This dramatically decreases the overall cost for the same capability as you could have on a stand-alone bus. While this saves significant amounts of money, the government customer can still have complete control over the payload. In addition, a hosted payload on a commercial satellite provides government planners with access to multiple launches each year in a variety of orbital locations, providing much needed flexibility in terms of timing, location and types of payloads. All of these factors make deployment of capability faster and more cost-effective. ✯

NEXT ISSUE

May 2012
Volume 16, Issue 4

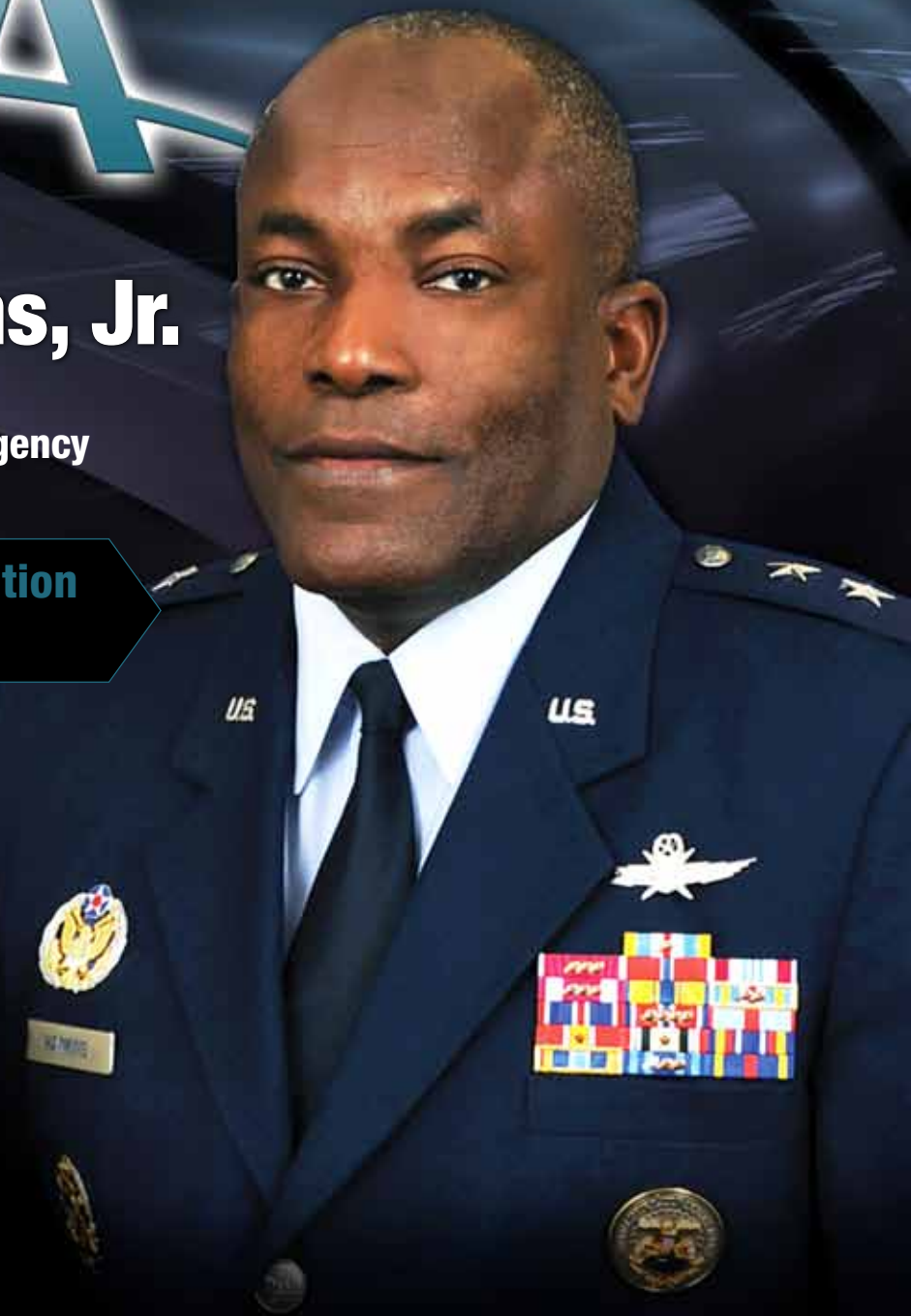
Military Information Technology

DISA

Cover and In-Depth Interview with:

Lt. Gen. Ronnie Hawkins, Jr.

Director
Defense Information Systems Agency



Annual Defense Information Systems Agency Issue:

- DISA 2012 Contracts Guide
- Reports on Key Programs
- Distributed at DISA Mission Partner Conference, May 7-10, 2012, Tampa, Fla.

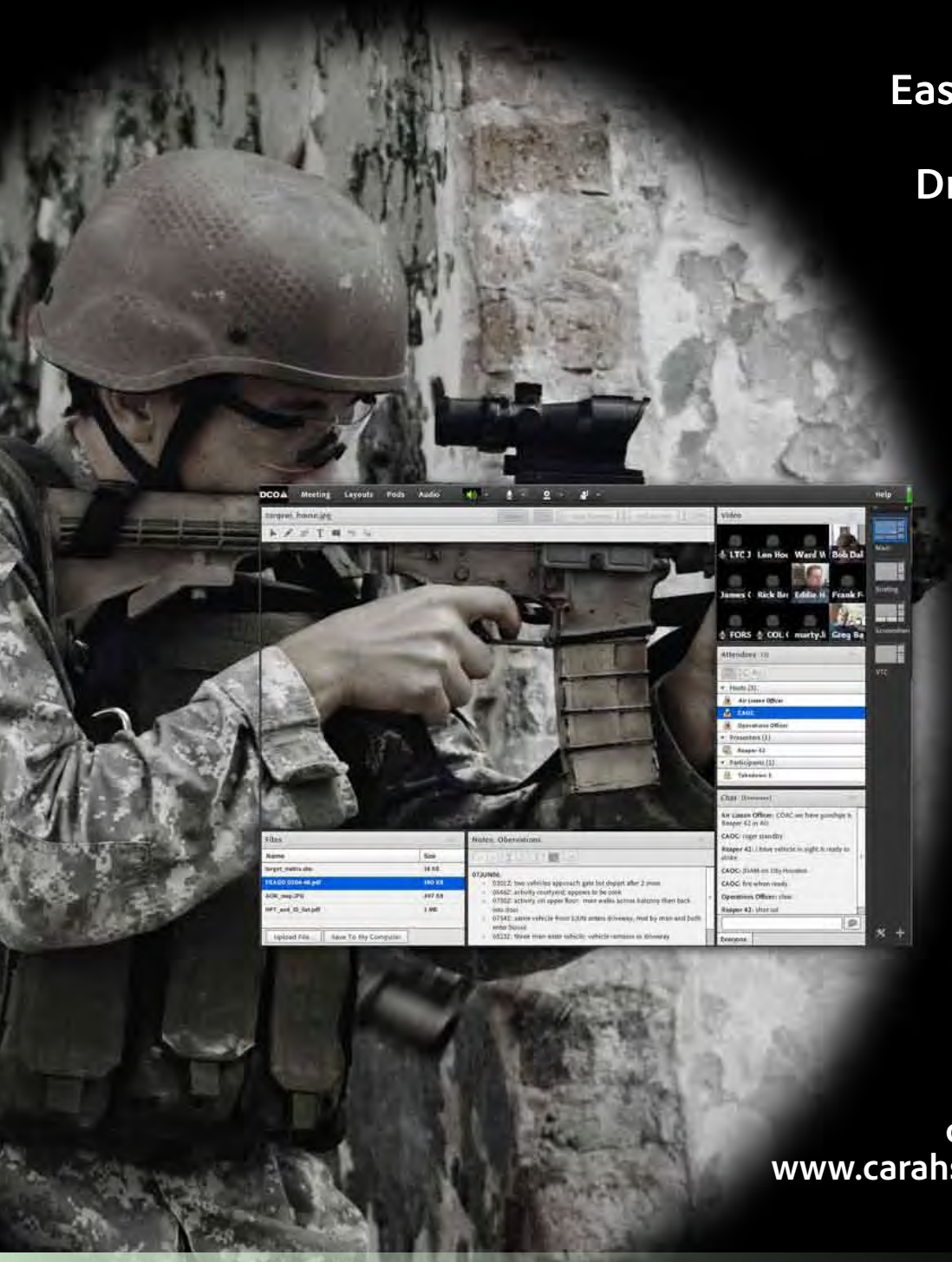
Features

- Tactical Networks
- STIG Compliance
- Agile Army Acquisition
- Data Center Consolidation
- Interoperability Expert

Insertion Order Deadline: **April 13, 2012** • Ad Materials Deadline: **April 20, 2012**

DCO IS UPGRADING!

Adobe



Easier to use interface

Drag-&-drop sharing

PDF support

Improved video

Create your own custom pods

Improved smartphone/ tablet capabilities

Tabbed chat… and much more.

DCO is upgrading to Adobe Connect 8.2!
Get a sneak peak of what's coming here: www.carahsoft.com/dco/upgrade/

Find out what half a million DoD users already know…

Communicate and collaborate for free with Defense Connect Online

DCO DEFENSE CONNECT ONLINE

Powered by Adobe® Connect™

https://www.dco.dod.mil/