ARMY TECHNOLOGY

U.S. ARMY RDECOM®

OCTOBER 2013 | VOLUME 1, ISSUE 2

A publication of science and technology news from the U.S. Army Research, Development and Engineering Command

FOCUS: CYBERSECURITY

+PLUS

INTERVIEW WITH

LT. GEN. EDWARD C. CARDON

ROTHTEC®

699 Tarkiln Hill Road New Bedford MA 02745
508 995 4601 hcarvalho@rothtec.com
www.rothtec.com

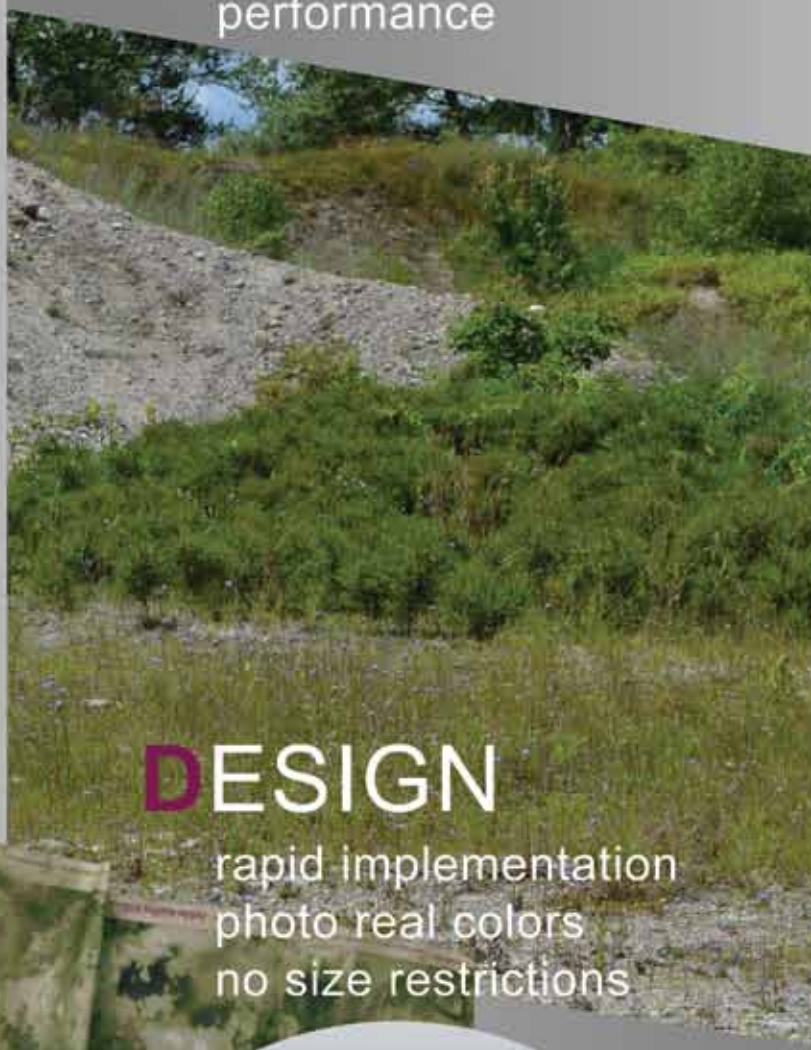
DIGITAL PRINTING

- Berry Compliant
- Veteran Owned Small Business
- Continuous operation since 1940
- Evolving digital technology since 1995
- Innovative R&D for DOD contracts since 2008
- Army SBIR Achievement Award Winner

"Rothtec,recognized for it's project ... making site specific camouflage clothing and equipment an operational reality."
-Army SBIR Newsletter, July 2012

RESEARCH

site specific
photo realistic basis
performance



DESIGN

rapid implementation
photo real colors
no size restrictions

PRODUCTION

colorfast
unique fabric capabilities
no minimums
commercialization

Rothtec Engraving Corp. wishes RDECOM & Army Technology future success

OCTOBER 2013 | VOLUME 1, ISSUE 2

IN THIS ISSUE

FEATURES

DEPARTMENTS

ACRONYM GUIDE

RDECOM	Research, Development and Engineering Command
AMC	U.S. Army Materiel Command
AMCOM-LCMC	Life Cycle Management Command
AMRDEC	Aviation and Missile Research, Development and Engineering Center
ARCYBER	U.S. Army Cyber Command
ARDEC	U.S. Army Armament Research, Development and Engineering Center
ARL	Army Research Laboratory
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics and Technology
CERDEC	Communications-Electronics Research, Development and Engineering Center
CISD	ARL Computational and Information Sciences Directorate
ECBC	Edgewood Chemical Biological Center
GSS	TARDEC Ground System Survivability
I2WD	CERDEC Intelligence and Inforamtion Warfare Directorate
NSRDEC	Natick Soldier Research, Development and Engineering Center
TARDEC	Tank Automotive Research, Development and Engineering Center
USAG Natick	U.S. Army Garrison Natick
USCYBERCOM	U.S. Cyber Command
WDI	AMRDEC Weapons Development and Integration

RDECOM works every day to make the Soldier's kit obsolete and enable our Army to enjoy an overmatch with our adversaries. But new technology also presents new threats. In the cyber world, maintaining an edge in security and capabilities requires an intimate understanding of the fundamental science behind computer networks.

As the Army strengthens its cyber defense and grows more nimble in cyber operations, our experts recognize how data is critical to dominance on the battlefield. What we do in cybersecurity is critical to the operation of the Army's networks, both tactical and fixed.

At RDECOM, we provide the Army with the necessary tools, techniques and capabilities in the field of cybersecurity.

In this issue of *Army Technology* magazine, we'll draw back the curtain a little to show how our scientists are delving into game theory to better understand opponents, strategies and rewards.

At the Army Research Laboratory at Adelphi, Md., our researchers are on the leading edge of new technologies like quantum data teleportation. In the future, computers will be vastly more complex and yes, even more intelligent. We talk with two senior ARL scientists about how they are shaping foundational research and development. (See page 6)

How computers interact in a mobile tactical environment is the domain of our Communications-Electronics Research, Development and Engineering Center at Aberdeen Proving Ground, Md. CERDEC researchers partner with Program Executive Offices, the Training and Doctrine Command, Cyber Command and ARL to develop solutions that are put into practice almost immediately.

Our experts are also drafting a cyber strategy that will help the Army prioritize and invest for the future. (See page 9)

We value our partners. The U.S. Army Cyber Command taps RDECOM scientists and engineers as the technical expertise for mission accomplishment. Lt. Gen. Edward C. Cardon, who took command last month, gives us his vision for the future of Army cybersecurity. (See page 4)

RDECOM is uniquely positioned on the leading edge of cybersecurity not only for the Army, but across the government. Our scientists and engineers have state-of-the-art skills that span the spectrum from developing hardware and software to integrating those systems into larger systems for users from the intelligence community to the Soldier on point in the field.

In addition, we have a host of partnerships in cybersecurity research and with other government agencies. We work with the Cyber Command, the National Security Agency, the Federal Bureau of Investigation and other agencies because in such a complex and rapidly changing field we have to share information, ensure a unity of effort and support other agencies when one of the capabilities we develop for Soldiers can help them. We also use the expertise of these agencies to help us make sure that what we're developing will meet the challenges our Soldiers are likely to face. This has long been the case in time of traditional war, and we are extending it to the borderless, intangible landscape of cyberspace.

October is National Cyber Security Awareness Month. We recognize that we are part of a larger effort to develop solutions to keep America's information safe and secure. Emerging cyber threats require engagement from the entire American community. RDECOM stands ready to meet the challenge.

Dale A. Ormond
Director, RDECOM

facebook.com/mrdaleormond

twitter.com/DaleOrmond

Bio http://go.usa.gov/vK8

We're always looking for good ideas to help keep our Soldiers safe. If you would like to submit a research or business proposal, business idea, recommend improvements to existing equipment or have a revolutionary idea that may be of benefit to the U.S. Army, please contact:

U.S. Army Office of Small Business Programs
Army Office of
Small Business Programs
106 Army Pentagon,
Room 3B514
Washington, DC
20310-0106

T: (703) 697-2868
F: (703) 693-3898

ARMY
TECHNOLOGY

EDITORIAL STAFF

Dale A. Ormond, RDECOM Director
Command Sgt. Maj. Lebert O. Beharie, Senior Enlisted Advisor
Joseph Ferrare, RDECOM Public Affairs Officer, (410) 306-4489
David McNally, Managing Editor, david.mcnally@us.army.mil

RDECOM ON THE WEB

http://www.army.mil/rdecom

SOCIAL MEDIA

http://about.me/rdecom

PUBLISHER

Carol Ramirez, Command Publishing
carol@command-publishing.com, (301) 938-8364
Kirk Brown, VP Sales and Marketing
kirk@command-publishing.com, (301) 938.8363

Army Technology Magazine is an authorized, unofficial publication under AR 360-1 for all members of the Department of Defense. Contents of U.S. Army Technology Magazine are not necessarily the official views of, or endorsed by the Department of the Army, the Department of Defense or the U.S. Government. The mention of a commercial product, service or firm is not meant to imply endorsement of that product, service or firm. The appearance of advertising in this publication, including inserts and supplements, does not constitute endorsement of products or services advertised by the Department of the Army or Command Publishing. The publication is printed by Command Publishing, a private firm in no way connected with the U.S. Army, under exclusive written contract with the U.S. Army Research, Development and Engineering Command. All editorial content is prepared, edited, provided and approved by the Public Affairs Office. Command Publishing is responsible for commercial advertising. Everything advertised in this publication shall be made available for purchase, use or patronage without regard to race, color, religion, sex, national origin, age, marital status, physical handicap, political affiliation or any other non-merit factor of the purchaser, user or patron. A confirmed violation of this policy of equal opportunity by an advertiser will result in the refusal to print advertising from that source. This magazine is printed on recycled paper with vegetable ink and is recyclable.

Ace Electronics
DEFENSE SYSTEMS

ELECTRONICS YOU CAN TRUST

Ace Electronics Defense Systems is a privately owned, Service Disabled, Veteran-Owned Small Business (SDVOSB). We began our company as a way to give the proper focus and attention needed to fulfil the detailed requirements of our military customers. We excel in the design, testing, and building of wire harnesses, cable assemblies, electro-mechanical box builds and diagnostic repair/integration services at our specialized, high-tech facilities for a wide range of military uses.

We at Ace Electronics Defense Systems pride ourselves as being 100% committed to meeting your needs by offering the highest quality manufacturing and engineering services available. We also have the satisfaction of providing these solutions in the most timely and cost effective manner possible.

Our customers have come to rely on us to present them with the proper guidance on manufacturing a suite of durable, secure and reliable products. We've been an integral supplier to our military customers, including RDECOM, for over a decade.

We're not just an electronics manufacturer; we're your primary partner in producing the best electronics possible in order to survive the rugged life-span of today's military programs.

MANUFACTURING | IT SERVICES | INTEGRATION | ENGINEERING | DESIGN

443-327-6100 | www.AceElectronics.com

Made in the USA

CERTIFICATIONS: ISO 9001, ITAR, IPC-A-610, IPC-A-620, J-STD-001, UL

Cage Code: 5TWH2

Service Disabled Veteran Owned Small Business
SDVOSB
cVE

Moving to the Future

INTERVIEW WITH LT. GEN. EDWARD C. CARDON, COMMANDER, U.S. ARMY CYBER COMMAND

The U.S. Army Cyber Command conducted its first change of command Sept. 3, at Fort Belvoir, Va., during a ceremony in which Lt. Gen. Rhett A. Hernandez, outgoing commanding general, relinquished command to newly-promoted Lt. Gen. Edward C. Cardon.

The Army activated ARCYBER Oct. 4, 2010, with a mission to plan, coordinate, integrate, synchronize, direct and conduct network operations and defense of all Army networks.

Cardon said he plans to pick up where Hernandez left off, and is honored to take command of ARCYBER.

"Army Cyber Command was borne out of the recognition of the tremendous convergence of technologies over time that created a new domain," he said. "As military cyber professionals, we must continue to strive to stay atop our profession. We are where we are today because of the tireless dedication of some of our most selfless and committed cyber leaders—these men and women have ventured into an entirely new frontier."

In one of his first media interviews since taking command, *Army Technology* magazine asked about future cyber challenges.

Cardon: Cyberspace offers both opportunities and challenges as our Army moves to the future. In a domain that is increasingly competitive and contested, we face a wide variety of formidable adversaries from nation states and extremist groups, to cyber criminals and individual hackers, and even insider threats, all of which pose grave danger to our networks, information, and overall readiness.

This rapidly growing body of actors is also increasingly adaptive, agile, flexible, and innovative operating within the domain. Fortunately, so are we. Within Army Cyber Command we are addressing three of our most pressing challenges to position our Army well for the future:

Building Cyber Capability and Capacity. In support of Joint and Army warfighters, we have begun an ambitious program to build teams that are trained, certified, equipped, and prepared to operate decisively throughout cyberspace. The building of these cyber teams marks the most critical action we are focused on today that can impact our future Army. Failing to recruit, train, and retain highly-skilled people at sufficient numbers to address a growing body of adversaries will put future Army formations at serious risk.

Transitioning to a More Defensible Platform. Commanders require a network that is capable, reliable, and trusted. Future networks must be joint, interoperable, agile, flexible, resilient and secure. We are working closely with DISA and USCYBERCOM to ensure the design and development of the Joint Information Environment [JIE] provides commanders at all levels a truly defensible cyber platform, capable of enabling a full range of cyberspace operations.

Gaining Situational Awareness in Cyberspace. The foundation in all military operations is our ability to know and understand ourselves, the enemy and the environment. In cyberspace, situation awareness depends on considerable amounts of relevant data sources and advanced storage and analytic capability, all intrinsically linked to our common cyber platform, JIE. We have built unstoppable momentum with USCYBERCOM and our sister services to include situational awareness into initial JIE designs, ultimately delivering a common operational picture to enable mission command and informed decision making. This will ensure we can visualize and protect terrain in cyberspace, particularly key terrain, thus denying our enemies access to their objectives. Given an increasingly congested domain, ensuring our ability to see ourselves offers a critical competitive advantage.

Q: What do you expect from Army scientists and researchers?

Cardon: Army researchers and scientists have always fulfilled an essential role in maintaining a vital and decisive technological advantage over our adversaries. However, new and unique challenges associated with this domain will test our ability to outpace our increasingly innovative and effective adversaries. Adversaries unable to compete in traditional warfighting domains can easily exploit a lower cost of entry and/or leverage criminal elements willing to share significant capability for relatively low costs. Now more than ever, the Army's scientists and researchers are uniquely positioned to shape the future cyber environment, ensuring the security of our networks and systems and enabling successful unified land operations.

Given the dynamic nature of cyberspace, predicting future technologies, developing innovative approaches and solutions, and aligning limited resources with the most fruitful long-term investments is both an extraordinary challenge and enormous opportunity.

I expect the Army's tremendous R&D community, along with its effective network of government, academia and industry partners, to understand operational challenges in cyberspace, solve our toughest challenges, and ultimately ensure the Army retains decisive technological and competitive advantages as it operates in the cyberspace domain.

The advantage in cyberspace will clearly belong to those that can gain, exploit, and protect advantages in this highly contested domain. Commanders at all levels will require the freedom to operate and maneuver in cyberspace, no longer content or permitted to view cyberspace as simply a medium for communications. As we progress within the Department of Defense toward the Joint Information Environment, it is imperative that we design and engineer foundational capabilities to deliver advanced cyber defense and shared situational awareness down to the tactical edge. And to be truly transformative, JIE must be the operational platform from which commanders can conduct decisive operations. Achieving such a transformative vision from the current state hinges on our ability to adapt our processes in the operational and R&D communities, tearing down formerly isolated efforts and capitalizing on the power of collaboration.

In an increasingly resource constrained environment and as we transform operational organizations and process, the R&D community will play a fundamental role in ensuring the cyberspace integration necessary for the Army's continued dominance on the battlefields of the 21st century.

Q: How knowledgeable should Soldiers, Army civilians and our contractors be in Cyber defense? What do you want the force to know?

During his 31 years of service, Lt. Gen. Edward C. Cardon has served in numerous key field and staff assignments. Before assuming leadership at ARCYBER, he commanded the 2nd Infantry Division.

Newly promoted Lt. Gen. Edward Cardon (left) accepts the ARCYBER colors from Army Chief of Staff Gen. Raymond Odierno September 3, 2013, at Fort Belvoir, Va. (U.S. Army photo by Dani Kyle)

Cardon: The creativity, innovation, and the wealth of the United States led to the development of computers and the growth of the Internet. Correspondingly, few segments of our society have benefited more from the expansion and integration of cyberspace than our military and specifically, our Army.

Across the warfighting functions, from command and control to intelligence to logistics, our combat advantage and equally our reliance on cyberspace has grown immensely. Cyberspace evolved quickly into a contested domain in which maintaining our comparative advantage requires an increasingly informed base of Soldiers, Army civilians, and contractors that understands the cyberspace threats and risks.

The Cyber threat is real. Even the most sophisticated cyber defense technology will be rendered ineffective and bypassed if users at every level are not an active aspect of our defense. Our success in operationalizing cyberspace depends upon the total force understanding the criticality of defending our networks from exploitation, disruption, and destruction.

Across our Army, everyone must increase their basic cyber awareness. We must expand our understanding of cyberspace threats, vulnerabilities and capabilities and then focus on our actions that expose our networks to risk. Adhering to basic cyber and information assurance policies that emphasize anti-virus protection and patch compliance, strong passwords and two-factor authentication, and the elimination of non-approved removable media usage will safeguard us against 80 percent of all known threats in cyberspace.

Fundamentally, leaders must offer the same amount of attention to assessing and mitigating risk across our networks as they would to any weapons platform. We must rely on continued strong training, leader development and education programs to further enhance operating safely in the cyberspace domain. ■

NAVARRO

Navarro is an award-winning, woman-owned, small business committed to excellence of services and customer satisfaction.

Proudly serving the U.S. Army as the Operations and Maintenance Contractor at Rocky Mountain Arsenal (RMA)

Navarro provides the following services to Federal clients nationwide:

- Facilities Management
- Operations and Maintenance
- Environmental Compliance
- Environmental Remediation
- ES&H/QA
- Research and Development
- Renewable Energy/Energy Efficiency
- Waste Management

Navarro Research and Engineering, Inc. ♦ 669 Emory Valley Rd., Oak Ridge, TN 37830 ♦ (865) 220-9650 ♦ www.navarro-inc.com

«CYBER R

Army cyber research lays foundations for future security

BY DAVID MCNALLY, RDECOM PUBLIC AFFAIRS

Growing threats in cyberspace threaten American national security. As the U.S. Army improves its defenses and the nimbleness of its response, scientists and engineers focus on understanding the underlying science of how networks operate; defending and developing technology solutions to keep them operational.

At ARL, Dr. John Pellegrino is director of the Computational and Information Sciences Directorate. He says by understanding the fundamental science behind cyber, the lab impacts the Army's overall network security.

"In the area of cybersecurity defense, we have extensive experience, but the science of cyber is not well understood," Pellegrino said. "We want a deep understanding of the science of cyber that could be applied to Army applications."

Dr. Alexander Kott, ARL CISD associate director for science and technology, uses a simple analogy.

"People have been building bridges since cavemen were around. The Romans were amazing bridge builders, some of those bridges are still standing today. But the first comprehensive publication about bridge design didn't appear until the mid-1850s. It then became possible for many experts to build bridges that would span great distance, withstanding the forces, as they had done in centuries past."

After engineers documented the scientific theory behind bridge building, the world saw amazing bridges blossom all over the world, Kott said.

"Likewise, people were building steam engines well before anyone knew about thermodynamics," Kott said. "First, they were building steam engines by trial and error. Then, after many empirical observations, someone said, 'I see the fundamental principles of how it all works together.' That scientific insight made it possible to build better engines."

NETWORK DEVELOPMENT AND EVOLUTION

"How can one mathematically describe a network?" Pellegrino asked. "How the network can evolve? How does it change as the number of nodes in the network increases? We try to understand how data can be moved around in different ways to engender the best protection."

CYBERSECURITY COLLABORATIVE RESEARCH ALLIANCE

The Army announces the Cybersecurity Collaborative Research Alliance with six partners embarking on a five-year venture. **BY ARL PUBLIC AFFAIRS**

Cyber security is critical to protecting Army systems from sophisticated attacks on military networks in the face of ever increasing importance of cyber systems.

ARL announced a newly forming Collaborative Research Alliance, or CRA, with six technology partners from government, academia and industry, which will explore the basic foundations of cyber science in the context of Army networks.

The partners who make up ARL's newest CRA will be formally announced this fall.

The Army will fund the alliance for five years at $2.5 million to $3 million annually with an option to renew for another five years.

"We generally enter into these kinds of alliances with complex problems in mind," said Dr. John Pellegrino, director of ARL's Computational and Information Sciences Directorate. "The fundamental science of cyber security is a long-standing challenge that will take a long time to solve."

The Army's goal is to bring in experts with varying perspectives to gain a deep theoretical understanding that would lay the groundwork for future Army solutions in cyber security, Pellegrino said. "It is what we call 6.1, or basic research."

ARL has identified three interrelated aspects of cyber security to explore and a cross-cutting psychosocial perspective that takes into account the human element of the network.

The study of the human element is a particularly distinctive aspect of the research, Pellegrino said. Each of the three research focus areas—named Risk, Detection and Agility—must take into account the people behind the cyber actions—human attackers, cyber defenders and end users.

ESEARCH»

As researchers begin to understand the fundamental limits on information transfer, they also recognize that hardware changes at an exponential rate, as do algorithms for network protocols.

"An interesting biological analogy is that humans are full of germs, viruses and bacteria," Kott said. "Perhaps we need to think about our computers similarly with inevitable viruses and malware. Just like people live with organisms and can be quite healthy, we need to get to that point of understanding with our artificial creations, computers and networks. Yes, you can penetrate computer networks. That's inevitable. But, we can accomplish the mission in spite of it."

NETWORK CONVERGENCE

In today's Army cyber landscape, there is a tactical network and a fixed network. CERDEC and ARL give special attention to the tactical network and its protection.

"For the fixed network, we can apply some degree of what's happening in the commercial sector," Pellegrino said. "This doesn't apply as much in the battlefield network because of mobility issues."

"Also, the threats tend to be different," he said. "There's some overlap. We can use some things, but other things we can't. The underlying science that can deal with the fixed networks is one thing. Then you have to look at it a little differently in those dynamic mobile tactical networks. That's where we are."

Cyber is an ever-expanding field of study with new technologies developed and implemented almost daily.

"We should probably not forget that the Army, even today and more so in the future, will have highly converged networks where tactical and strategic really become one and the same, and there's less of a distinction between them than there is today," Kott said. "There is a need for a broader science, a broader understanding and broader theoretical foundations for insights into such converged networks."

PARTNERSHIPS

RDECOM organizations develop cyber security solutions in close coordination with the U.S. Army Cyber Command, known as ARCYBER.

"Army Cyber Command has made great progress and will continue

Dr. Alexander Kott, ARL CISD associate director for science and technology explained the three research areas this way.

The first area, Risk Research, seeks to develop theories and models for dynamic risk assessment and explores risk-related fundamental properties of dynamic cyber threats, Army networks and defensive mechanisms.

The next, Detection Research, should shape cyber threat detection and recognition capabilities that inform approaches to rapid adaptation of a detection technique or algorithm as new cyber threats emerge on the battlefield, he said.

And finally, he said, Agility Research supports planning and control of cyber maneuvers, which are ways to rapidly adjust our networks and defenses in order to defeat or mitigate cyber threats and effects.

"When we talk about a collaborative research alliance, one of the key values of this mechanism is that we are educating the academic community in the types of problems and unique challenges that the Army needs to have addressed," Kott said. "We are influencing and guiding the research community toward developing research skills particular to that niche."

Similar alliances exist at the lab for collaborative research in advanced electronic materials and materials in extreme dynamic environments, Kott said.

In the case of cyber security, ARL has had a strong internal program for years, in part to defend the Army supercomputing resources. The ARL Supercomputing Research Center had a ribbon-cutting earlier this year to mark an expansion and greater high-performance in-house computing capability, Pellegrino added.

But new, evolving cyber challenges require an even deeper look into the foundation of the problem. Technical leaders are preparing for the Army of 2020 and beyond.

Future Army networks will be heterogeneous and convergent, comprising a wide variety of fixed wired networks, mobile cellular networks, and mobile ad-hoc networks, he said.

The dynamics, scale and complexity of Army networks coupled with evolving, advanced, persistent threats makes cyber security a grand challenge that will require multi-disciplinary experts working together, Pellegrino said.

Although we expect pockets of near-term results that we could apply rapidly, this alliance is a long-term commitment to laying a framework towards solutions into the future 10, 15 and even 20 years away, he said.

to remain trained and ready to ensure our forces maintain our freedom to operate," Lt. Gen. Rhett Hernandez said in testimony before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities last year. Hernandez stood up ARCYBER and served as its first commanding general. During his tenure, he instituted a partnership with RDECOM.

"We're focused on providing a professional team of elite, trusted, precise, disciplined cyber warriors who defend our networks, provide dominant effects in and through cyberspace, enable mission command, and ensure a decisive global advantage," he said.

To meet that focus, ARCYBER's relationship with researchers has grown Armywide.

"We have a strong partnership," Pellegrino said. "ARL and CERDEC have complementary goals with ARCYBER. Together we serve as the technical consultants and provide the technical basis for the command."

One result has been a cyber security training program for the U.S. Army Reserves and National Guard.

Another important partnership, this one between ARL and the U.S. Cyber Command, known as CYBERCOM, produced an initiative in the development of cyber security training for the U.S. Army National Guard.

"CYBERCOM initiated that relationship," Kott said. "They looked at some of the capabilities and tools we have developed at ARL and asked, 'Can you take that experience and help train the National Guard?' CYBERCOM approached the Bureau of the National Guard and said, 'You need to talk to ARL, and they will help you to get trained on computer network defense,' which is very relevant to some of the missions the National Guard have."

Pellegrino said AMRDEC also collaborates with ARL.

"Our workforce is fairly small," he said. "We partner across RDECOM, and apply the expertise."

ARL's ultimate mission is to develop knowledge.

"But then we need to share that knowledge, and that sharing takes multiple forms … transferring technology to another RDEC, helping an operational entity like ARCYBER, training cyber warriors … so we do all that," Kott said.

ARL is also establishing a Cybersecurity Collaborative Research Alliance that will include up to six partners from the defense, academic and industrial communities.

GAME THEORY

Army researchers use game theory to understand potential computer security solutions. Game theory is a collection of mathematical formulations used to understand and develop strategies in disciplines ranging from economics to biology.

"We frequently see a race between security and network attackers. One day an intelligent solution is proposed to fix a problem, and the next day the attackers come up with a smarter way to circumvent the proposed countermeasure," Pellegrino said.

Game theory may help explain what happens in cyber security interactions, which involve opponents with conflicting goals.

"When playing a game of Risk or Monopoly, there are interactions between players that occur," he said. "There is research in the mathematical community that has formulated those interactions, and described them in mathematical terms, when one is trying to out-think, out-smart the other. They move information around to essentially play 'keep-away.'"

Game theory provides mathematical descriptions of players' actions, payoffs and strategies, Kott said.

The Army is also figuring time and relevance of information into the cyber security equation.

"We know that certain types of information—if our adversaries know it—won't be useful to them because of time constants," Kott said. Pellegrino says the prevalent thinking is that all data must be secured and locked down.

Learning how to quantify risk in networks is a big deal. How do we quantify risk? We need to be able to tell commanders the options available to them and explain the risk of vulnerability—10 percent, 20 percent, 30 percent—with these approaches."

In the near future, commanders will be able to use this information to assess the appropriate level of risk and apply it to scenarios or missions.

LEAP-AHEAD TECHNOLOGIES

Soon after taking office in 2009, President Obama identified cybersecurity as "one of the most serious economic and national security challenges we face as a nation."

One goal of the White House initiatives is to develop technologies that provide increases in cybersecurity by "orders of magnitude above current systems" and that can be deployed within five to 10 years.

ARL researchers are on the leading edge of exploring new solutions.

"Quantum communications offer interesting opportunities for securing the transmitted information—or at least knowing whether an adversary has touched those communications," Kott said.

ARL is pioneering data teleportation and hopes to send information from one location to another without the data being transmitted through the intervening space.

"One day we will have communication over worldwide distances with quantum repeaters as mediators at nodes in between," ARL physicist Ron Meyers said. "We'll be able to teleport information globally. What we'll have is tamper-resistant security."

CONCLUSION

The state of our knowledge about cyber security world changes quickly, and the line between fundamental science and research and its application is razor thin, Pellegrino noted.

"We discover new things every day. As we discover them, we try to insert them into practice, and make use of them to the maximum extent possible," Pellegrino said.

Cyber is a problem that will not be solved overnight.

"The problems associated with understanding the related parameters, and the fundamental science of networks and network security, is a huge issue that is not going to be solved in 15 minutes," Pellegrino said. "Nor does anyone think there is going to be a major breakthrough that all of a sudden makes everything clear. That's unlikely to be the case. We believe a concerted long-term focused effort, coupled with taking and applying the findings that we have as soon as they occur, is the strongest approach that we can pursue." ■

DELIVERING THE ARMY CYBER STRATEGY

Defining the Army's top cyber priorities and the way forward

BY KASHIA SIMMONS, CERDEC PUBLIC AFFAIRS

Army computer scientists and engineers predict that the future of warfare may be primarily digital within the next 30 years. In a detailed cyber strategy document now in final draft, CERDEC officials hope to provide a solid foundation for Army planners.

The goal of the strategy is to define the Army's top cyber priorities and a way forward for wise future investments, said Henry Muller, the Army lead tasked to spearhead the planning effort, and director of the Intelligence and Information Warfare Directorate of RDECOM's communications-electronics center, or CERDEC I2WD.

"We had to cover everything from doctrine to R&D; acquisition through sustainment," Muller said. "We knew it was going to be a pretty tough job and that there wasn't total consensus for cyber capabilities for the tactical Army, but we needed to understand where the Army wanted to go with respect to cyber on the battlefield—and cyber in general, and try and shape how we would make investments. That came together as part of this plan."

While the Army has many of the same cyber challenges as the other services, there are some significant peculiarities. More so than the other services, the Army has a large tactical footprint on the battlefield, which places them in close proximity to its adversaries, Muller explained.

"That represents a threat from a cyber defense standpoint, but also an opportunity from an offensive cyber perspective, and I thought, 'that's why we needed to sit down and try and figure out how we go forward with that,'" Muller said.

The initial goal was to develop a strategy for the future of Army cyber to the year 2048. The task force began by conducting analysis on the current force and network as it stands today and how they are predicted to evolve in the coming years.

Although this provided a solid foundation, attempting to predict the cyber environment 35 years into the future proved unreasonable in such a dynamic realm as the cyber domain, and the task force decided to narrow the scope of the strategy.

"This first go around we're not going to get out to 2048; we'll go out to around 2020 or so. One of the surprises, I guess, was we put an RFI [request for information] out to industry to help us project into the future. And it really showed how reticent people are to try to predict too far out specifically in this technology area, which is predominantly IT," Muller said.

Another such area Muller said one could not project, though he expected considerable change, was in the policy surrounding cyber offensive operations on the battlefield.

"How we're going to conduct cyber offensive operations on the battlefield and what will be the authorities we ultimately operate within..." Muller said is what might change the most.

Muller's kick-off meeting for the Army Cyber Task Force was Dec. 13, 2012, and assembled senior Army leaders from the Army Capabilities and Integration Center, G2, G6, Army Cyber Command, and program executive officers from PEO Command, Control and Communications Tactical and PEO Intelligence, Electronic Warfare and Sensors to agree on a plan to develop the strategy.

"I made it very clear to everybody that in no way, shape or form did I think that I, Henry Muller, was here to define the Army cyber strategy—that the Army leadership, TRADOC and ARCYBER had to define the strategy and way forward and that what we wanted was to facilitate bringing all that together," Muller said.

Over the last 10 months, eight cross-functional project teams have worked to outline the key tenets of the Army's cyber strategy, the first draft of which was submitted to the full task force for review Aug. 8.

Muller emphasized the importance of collaboration across the Army and defense community as a key tenet for the success of the Army cyber strategy. When all is said and done, the strategy will determine where more work is required across the entire Army enterprise, to include doctrine, organization, training, materiel, leadership and education, personnel and facilities. It will define where acquisition programs are going, and what the Army strategy will be in order to better inform industry so they can plan how to best invest their corporate research and development dollars.

The final draft of the Army's cyber strategy is due to ASA (ALT) Oct. 31.

ARMY LAB INVESTIGATES "CYBER SCIENCE"

Can an evidence-based approach to secure networks lead toward a fundamental science of cyber security?

BY ARL PUBLIC AFFAIRS

An ARL Network Assurance Branch team member works on a series of cyber challenges at the Global CyberLympics World Finals last year. The lab's cyber defense team is responsible for delivering protection, detection, response and sustainment services to DoD customers. Photo courtesy of Global CyberLympics

U.S. Army Research Laboratory cyber defense team members compete in a cyber security challenge at the Global CyberLympics World Finals last year. On a day-to-day basis, they monitor networks of diverse agencies within the Department of Defense. Photo courtesy of Global CyberLympics

Scientists are skeptical about terms like "breakthrough" and "novel," but few things are more suspect than a claim of the birth of an entirely new science.

Nevertheless, terms like "Science of Cyber" have been popping up with greater frequency as technical intricacies of cyber security become better known, said Dr. Alexander Kott, ARL associate director for science and technology, Computational and Information Sciences Directorate.

ARL's portfolio of cyber research takes an evidence-based approach to define the elements within the field of cyber security as it relates to protecting and defending Department of Defense, or DoD, networks, to see if there is potential for emergence of "Cyber Science," Kott said.

As early as 2010, an independent group of scientists, which advises the U.S. government on matters of science and technology was commissioned by the DoD to evaluate whether a more scientific approach to cyber security would be possible.

The Jason Defense Advisory Group looked into, for example, whether metrics could quantify the cyber-security status of a system, a network or a mission, according to the 2010 report published by the Mitre Corporation.

The group found that connecting government, academia and industry to meet DoD's challenges would be an important step in nurturing scientific inquiry.

"ARL has years of experience monitoring DoD networks, and developing tools for intrusion detection and forensics," Kott said. "We work with a number of key partners to protect critical data."

In defining the domain of the science of cyber, ARL started with the threatening artifact, malicious software, and the resulting security incidents.

Scientists within the lab and others are in search of a coherent family of models that yields experimentally testable prediction of characteristics of security violations, Kott said.

For instance, one research effort at the lab is concerned with the architecture and approaches to detection of intrusions in a wireless mobile network. If software agents were deployed on computing devices of the wireless network, and sent relevant observations of the network traffic and of host-based activities to a central analysis facility, then it would provide a means for an analysis to comprehensively process and correlate the information, he said.

"There is a breadth of issues associated with systemizing the cyber research, like the need for a theory of algorithms that are likely to preserve the critical information indicating an intrusion," Kott said. "And we need a means of rigorously characterizing the detection accuracy."

Basic research at the lab delves into intrusion understanding, as well as network metrics, network sensors, trust management and advanced threats, Kott said.

The research of the science of cyber goes hand-in-hand to complement the lab's practical computer defense program, which helps answer cyber threats more proactively.

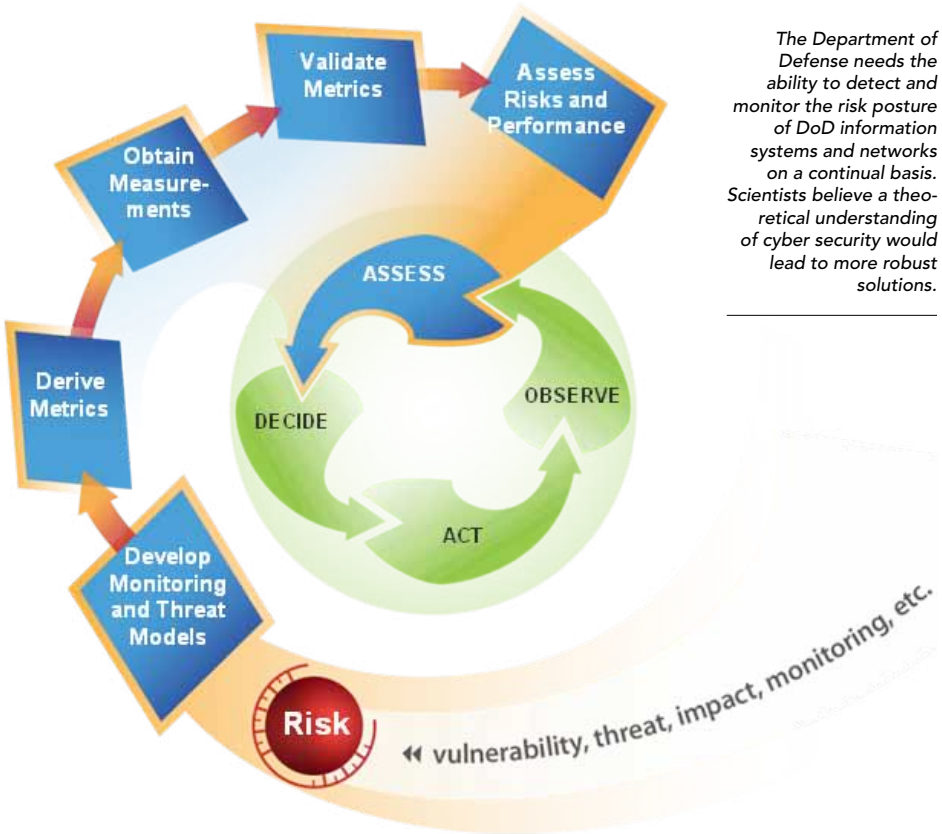
"The bridge between academia and industry enables us to leverage emerging ideas and technology to enhance the security posture of information systems connected to Soldiers," said William Glodek, team lead with ARL's Network Security Branch. "When Soldiers are in a tactical environment, compromise of a system or network could result in loss of life. It is a priority to protect Soldiers from the kinetic effects that can be delivered with help of cyber threats."

While network and information security policies and best practices have been established, we are starting to identify and fill gaps as new technology emerges. "But still we're working to get better," Glodek said.

"We have the luxury of working with cutting edge developmental technology that may be utilized in the mid- to far-term," he said.

Now and in the future, scientists from a variety of research fields have to grapple with the question of a scientifically rigorous approach to cyber security.

ARL will continue to look at the cyber security challenges of assessing vulnerabilities for defense networks, predicting upcoming risks and preventing attacks, responding with an empirically-based approach that "will make contributions to the larger question of 'is there a scientific basis behind cyber security?'" Kott said. ■

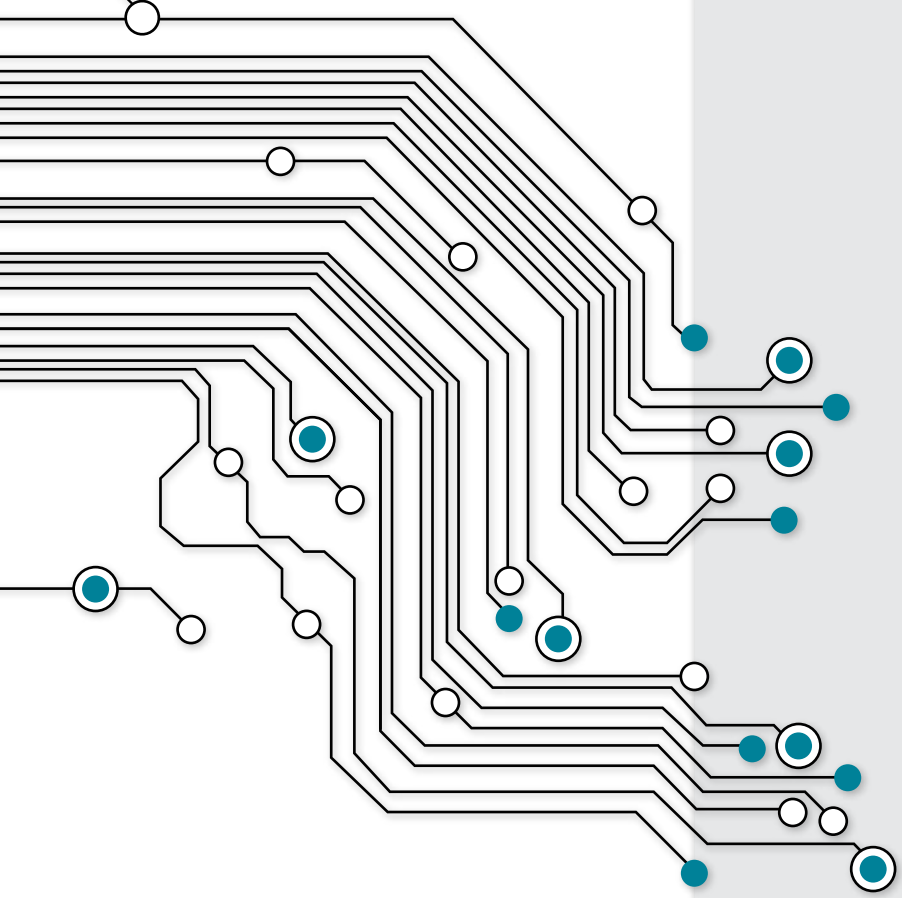


The Department of Defense needs the ability to detect and monitor the risk posture of DoD information systems and networks on a continual basis. Scientists believe a theoretical understanding of cyber security would lead to more robust solutions.

DEFINING NEXT-GEN PROTOCOLS AND ARCHITECTURES

The Army looks to blend cyber and electronic warfare capabilities on the battlefield

BY KRISTEN KUSHIYAMA, CERDEC PUBLIC AFFAIRS



As new technologies emerge and new cyber and electronic warfare threats plague Soldiers in the field, U.S. Army scientists and engineers continue to define next-generation protocols and system architectures to help develop technology capabilities to combat these threats in an integrated and expedited fashion.

As part of the Integrated Cyber and Electronic Warfare, or ICE, program, CERDEC researches the technologies, standards and architectures to support use of common mechanisms used for the rapid development and integration of third-party cyber and electronic warfare, or EW, capabilities.

"Currently, within cyber and EW disciplines there are different supporting force structures and users equipped with disparate tools, capabilities and frameworks," said Paul Robb Jr., chief of CERDEC Intelligence and Information Warfare Directorate's Cyber Technology Branch.

"Under the ICE program we look to define common data contexts and software control mechanisms to allow these existing frameworks to communicate in a manner that would support the concurrent leveraging of available tactical capabilities based on which asset on the battlefield provides the best projected military outcome at a particular point in time," Robb said.

The boundaries between traditional cyber threats such as someone hacking a laptop through the Internet, and traditional EW threats such as radio-controlled improvised explosive devices that use the electromagnetic spectrum have blurred allowing EW systems to access the data stream to combat EW threats, according to

Giorgio Bertoli, senior engineer of CERDEC I2WD's Cyber/Offensive Operations Division.

Additionally, significant technological advancements including a trend towards wireless in commercial applications and military systems have occurred over the last decade, said Bertoli.

"This blending of networks and systems, known as convergence, will continue and with it come significant implications as to how the Army must fight in the cyber environment of today and tomorrow," Bertoli said.

"The concept of technology convergence originated as a means to describe the amalgamation of traditional wired versus wireless commercial services and applications but has recently evolved to also include global technology trends and U.S. Army operational connotations—specifically in the context of converging cyber and EW operations," Bertoli said.

The Army finds itself in a unique position to help mitigate adverse outcomes due to this convergence trend.

"Post force deployment, the Army has the vast majority of sensors and EW assets on the tactical battlefield compared to any other service or organization posing both risks and opportunities. Our military's reliance on COTS [commercial-of-the-shelf] systems and wireless communications presents a venue for our adversaries to attack. Conversely, the proximity and high density of receivers and transmitters that we deploy can be leveraged to enable both EW and cyber operations," Bertoli said.

"The ability to leverage both cyber and EW capabilities as an integrated system, acting as a force multiplier increasing the commander's situational awareness of the cyber electromagnetic environment, will improve the commander's ability to achieve desired operational effects," Robb said.

A paradigm shift in how the Army views system and technology development will further enhance CERDEC's ability to rapidly adapt to new cyber and EW threats.

"The biggest hindrance we have right now is not a technological one, it's an operational and policy one," Bertoli said. "The Army traditionally likes to build systems for a specific purpose—build a radio to be a radio, build an EW system to be an EW system, but these hardware systems today have significantly more inherent capabilities."

To demonstrate the concepts of multi-capability systems, CERDEC chose not to solely focus its science and technology efforts on researching solutions to address specific cyber and EW threats but also to develop the architecture onto which scientists and engineers can rapidly develop and integrate new more capable solutions.

"As an example, the World Wide Web has grown into an architecture that is so powerful your tech savvy 10-year-old can build a website—and a pretty powerful one at that," Bertoli said. "The only reason this is possible is because there is a wealth of common tools, like web browsers and servers, and standards such as HTML or HTTP already in place for them to use."

"The ICE program is attempting to extend this model to the cyber and EW community by providing mechanisms to enable the leveraging of available tactical assets to support cyberspace operation mission sets. Early focus revolves around the development of augmented situation-awareness capabilities but will evolve to include the enabling of a multitude of cyberspace operations," said Bertoli.

ICE will provide the Army with common tools and standards for developing and integrating cyber and EW capabilities.

"Capabilities can be developed to combat EM [electromagnetic] and cyber threats individually, but this is neither time nor cost effective and simply will not scale in the long term. The domain is just too large and will only continue to expand," Bertoli said.

"In the end, we [CERDEC] believe this is the only way the Army will be able to keep pace with the anticipated technology advancements and rate of change related to cyberspace and the systems that comprise it," Bertoli said.

The Army acquisition community has also seen changes in the relationship between cyber and EW.

"Tactical EW systems and sensors provide for significant points of presence on the battlefield and can be used for cyber situational awareness and as delivery platforms for precision cyber effects to provide a means of Electronic Counter Measures and Electronic Counter-Counter Measures for instance," said Col. Joseph Dupont, program manager for EW under Program Executive Office Intelligence, Electronic Warfare and Sensors.

"There is no doubt in my mind that we must provide for a more integrated approach to cyber warfare, electronic warfare and electromagnetic operations to be successful in the future conduct of unified land operations," Dupont said.

CERDEC, as the Army's research and development experts in cyber and EW, works closely with the Program Executive Offices, the Army's Training and Doctrine Command and Army Cyber Command to shape operational concepts and doctrine by providing technical expertise regarding technically achievable solutions in the context of the tactical cyberspace operations and supporting materiel capabilities for the Army.

In addition to working with the Army's strategy and policy makers, CERDEC I2WD has tapped into its facilities and pre-existing expertise to further the ICE program.

CERDEC I2WD maintains state-of-the-art laboratories that support both closed and open air testing facilities to provide relevant environment conditions to conduct research that provides a seamless cyber-electromagnetic environment with both wired and wireless modern communication infrastructure.

"We leverage these facilities and our inherent core competencies in cyber, EW and signals intelligence to engage with the Army and the community at large, both academia and industry partners, to collaborate on developing and integrating relevant technologies to achieve domain superiority in a changing environment," Robb said.

The fully-instrumented labs include commercial information assurance products and allow for in-depth experimentation while sustaining automated rapid network re-configuration technology and virtualization technologies to support scalable testing. Additionally, I2WD expands its potential environment by maintaining remote connections with external government sites, which also enables collaborative experiments.

The combination of these assets and expertise allows CERDEC to demonstrate achievable capability improvements related to cyber and EW convergence.

"During the next three years, the biggest thing we can do within the ICE effort is show the art-of-the-possible by providing technology demonstrations on both existing and experimental Army systems to provide concrete proof of the advantages such a capability can provide," Bertoli said. ■

IMPROVING SITUATIONAL AWARENESS

615456-50 TACT R

615456-49 TACT R

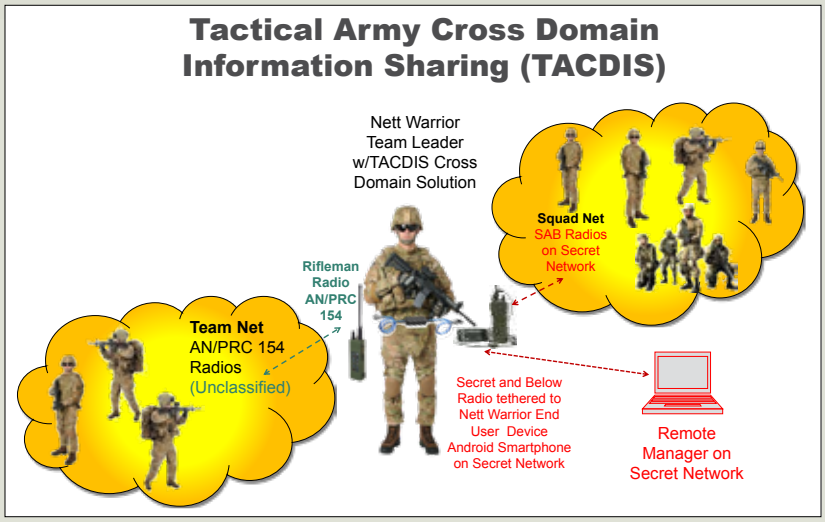
The Army links tactical networks for first time with new device

BY AMANDA ROMINIECKI, CERDEC PUBLIC AFFAIRS

For the first time, dismounted Soldiers using unclassified Rifleman Radios will be linked to the classified Nett Warrior system by a new cross-domain device, improving situational awareness on the battlefield while maintaining the security of both networks.

CERDEC engineers have developed a device allowing for the two-way sharing of information across tactical networks with differing security classifications, known as Tactical Army Cross Domain Information Sharing, or TACDIS, bridging the gap between a commonly used Army radio and a classified system for the first time.

The TACDIS program began in 2009 to meet the PEO Soldier need for cross-domain information sharing with the Nett Warrior system. Nett Warrior is the Army's classified handheld situational awareness and mission command system used by team leaders in combat operations, which needs to receive data from the unclassified Rifleman Radio in order to improve situational awareness on the battlefield.



TACDIS is used as a component of the Nett Warrior system, connecting the unclassified Rifleman Radio to the classified Nett Warrior system allowing for the secure incorporation of Soldier position information to improve situational awareness for both the Nett Warrior team leader and the commander.

Rifleman Radios used by dismounted Soldiers send out geographic location messages which can be used for improved situational awareness on the Nett Warrior system. However, information from unclassified radios cannot be transferred to a classified system without a cross domain solution like TACDIS to securely link them together, explained Philip Payne, CERDEC TACDIS program lead.

"In order for commanders to have higher granularity of where all his Soldiers are, to know where those dismounted, unclassified Soldiers are located, they need TACDIS," Payne said. "It incorporates more Soldiers, down to the tactical edge, and brings them into the classified common operating picture."

"It's kind of a natural fit that we [CERDEC] would work on cross-domain guards [like TACDIS]," said Dr. Paul Zablocky, director of the CERDEC Space & Terrestrial Communications Directorate. "We understand how to break them, how others would break them, so we can be sure that we design them and build them properly. And we understand how to interface them to the radios because we have the expertise on the radios."

That location information is transferred autonomously through the TACDIS device, eliminating any added burden on the Soldier associated with a new piece of technology. If the device is carried by the team leader as a component of the Nett Warrior system it will seamlessly share this critical unclassified information with classified networks, explained Payne.

"The TACDIS device, when properly integrated with the Nett Warrior system, will enable individual Soldier positions to be known," said Jeff Grover, Project Manager Soldier Warrior (PM SWAR) information assurance manager. "This improved situational awareness will decrease fratricide and increase mission effectiveness of infantry Soldiers."

The TACDIS device uses the AAMP7 microprocessor which has NSA certified security partitioning allowing for the secure transfer of information. Certification testing for the TACDIS device began in September at Fort Huachuca, Ariz., and will continue through early 2014. Certification is overseen by the NSA, ensuring information can be transferred safely while maintaining the security of the classified network.

After certification, the program will be transitioned to PEO PM SWAR, for developmental and field testing, large-scale production and eventually fielding to the operational environment, explained Payne.

"PM Nett Warrior will evaluate TACDIS in an operational setting during NIE 15.1 which is scheduled for October 2014," Grover said. "Following a successful NIE event, a production phase would be initiated to equip and train Nett Warrior Team Leaders."

According to Grover, if the program remains on schedule, fielding is expected to begin as early as 2015. ■

A football analogy to describe cyber security efforts

BY CERDEC PUBLIC AFFAIRS

Cyber experts Giorgio Bertoli and Stephen Lucas work together to provide offensive and defensive cyber capabilities for Army tactical operations from two directorates within CERDEC. Much of Bertoli's work focuses on the offensive tactics for cyber attack while Lucas' efforts aim to defend the network. To further illustrate both sides of the cyber landscape, Bertoli and Lucas explain their efforts in a head-to-head, football game: the "Cyberbowl."

Bertoli is an electrical engineer and computer scientist currently serving as senior engineer for the Information and Networks Operation division of CERDEC's Intelligence and Information Warfare Directorate. Bertoli has more than 18 years of combined Active military duty and civilian government engineer experience in electronic warfare, computer network operations and cyber-related technologies.

Lucas is an electrical engineer and is serving as the chief engineer for the Cyber Security and Information Assurance division of CERDEC's Space and Terrestrial Communications Directorate. Lucas has more than 25 years of civilian government experience in information assurance, communications security/transmission security, computer/network security and cyber defensive capabilities/technologies.

Welcome to the 2013 Cyberbowl championship where the Lucas Defenders are about to take on the Bertoli Hackers. Teams have practiced extensively and researched each other's vulnerabilities in the months leading up to this match. The Defenders have focused on message board postings on underground forums, newsletters, mailing lists and Internet relay chat rooms in order to learn what attacks and techniques the Hackers could have in their playbook.

Likewise, the Hackers have been engaged in researching available open-source information on the Defenders and their security posture, organizational structure and personnel. Something as seemingly innocuous as an organizational chart and an email list can provide valuable venues of attack for the Hackers.

It's kick off, and the game is on the way. It's first-and-10 on the 20-yard line and the Hackers take the field on offense. Looks like the Hackers are taking a conservative start to the game by running basic IP and port scans plays trying to better determine the Defenders security posture. Such activity isn't going to gain much yardage for the Hackers, but testing their opponent could reveal valuable information and help identify significant weaknesses in the Defenders' network architecture and security configurations.

It's second-and-7 after the Defenders only gave up 3 yards against the IP and port scanning play. They've lined up in a Firewall formation, this style of defense will allow the Defenders to monitor and close-off all the ports the Hackers could take through the line of scrimmage by closely investigating the communications in and out of their side of the field.

Third-and-short, the Hackers are now looking deep for an initial foothold within the Defenders' territory. By leveraging what they know about the Defenders' personnel structure and discovered email addresses, they are executing highly targeted "Spear Phishing" plays. Such attacks are very effective, (especially in highly hierarchical organizations) at fooling the defense into unwittingly assisting the offense.

The Hackers convert on third down and are now looking at a first-and-10 on the Defenders' 45. The Defenders' coaches can be seen on the sidelines instructing their players about proper email security, how not to fall for trick emails and trick plays, to trust email only from individuals they know and to always use an anti-virus to scan attachments before opening them. Back on the field the Defenders are trying an intrusion detection system approach that will allow them to closely inspect all packets and plays coming from the Hackers and look for anything that matches a signature in the Hackers playbook. The intrusion detection system defense will effectively shut down any play the Hackers have that the Defenders already know about.

It's been an evenly matched game so far, but the Hackers have gained some momentum in the last few plays and several Defenders are sidelined now due to email and web-based exploitation. Looks like the Hackers are now trying to cause even more damage and confusion by executing a broad range denial of service play. Such attacks are not very "high tech," nor are they stealthy, but they are very hard to defend against and can bring even a good defensive team to complete halt.

The Defenders seem to know a denial of service play is coming from the Hackers so they are planning to blitz by bringing up other servers in the "cloud" and configuring their downstream routers to drop all packets that are not coming from authenticated sources in an attempt to circumvent the denial of service.

The Cyberbowl's outcome is still to be decided, but the Hackers are determined to find new ways of overcoming their archrival Defenders. This matchup will be an exciting one for years to come as both sides continue their struggle to dominate the cyber landscape by leveraging new technologies and research. One thing is for sure, as a spectator, this is the game to watch! ■

The Need for Data

Data helps Army leaders with challenging manpower decisions BY DAVID VERGUN, ARMY NEWS SERVICE

Army leaders face challenging decisions regarding manpower, readiness and modernization as budget restrictions and uncertainties continue.

Now more than ever, leaders need data that is both reliable as well as understandable so they can make better-informed decisions on how and where to allocate their resources, said one of the Army's leaders in data management.

Commanders not only need to know the current state of unit readiness, they'd also like to know where those readiness levels will be in six months or 10 years, said Lt. Col. Bobby Saxon, division chief of Enterprise Management Decision Support, G-3/5/7.

It's a tall order, he admitted. Enterprise Management Decision Support, or EMDS, the system he manages, has only been operational since 2010.

Currently, the EMDS system draws from about five years of historical data and from about 20 databases. A lot of the data comes from the Defense Readiness Reporting System-Army and the Army Operations Directorate.

Business rules are then applied to the data to make it consistent and to present the material in the easy-to-understand format needed by the stakeholders—normally commanders and action officers.

In the near future, EMDS's capabilities will increase, Saxon said. "We're now laying the foundation for strategic readiness," he explained.

Strategic readiness is one of Chief of Staff of the Army Gen. Ray Odierno's priorities.

"There are two key components to that," Saxon said. "The first is the consumption of additional data. We consume data from dozens of data systems; in turn, those data systems pull data from other sources allowing EMDS, indirectly, to pull data from a much larger information reserve."

Saxon and his team recognize that more data can paint a better long-term picture.

"For example, we don't have a lot of funding data in our system today, but if we are going to look strategically into the future, one of the key factors will be how much money is planned for training, personnel, installations and equipment," he said. "This information will help us paint a more robust and accurate picture as we look out into the future."

The second piece of laying that foundation is the use of IT tools and making sure the Army has the right toolsets in place in order to tackle the task correctly, he said.

"We've reached across industry to get an idea of what's commercially available," Saxon said. "One of the things we do as an organization, any time we move forward, is cast a net as wide as possible in our fact gathering so we're not duplicating something that already exists or going down a much harder path then we should."

Strategic readiness means anticipating readiness levels in units, training, personnel, equipment and systems six months to 10 years or more in the future, Saxon explained.

To do that requires an enormous amount of historical and current data, he said.

HURRICANE-LIKE FORECASTING

Saxon likened the process to predicting a hurricane's strength and then tracking where it will make landfall. To do that requires a lot of sensors in the air and in the water to measure water temperature, wind speed and other factors.

In the case of a hurricane, those data points are fed into a computer model which can forecast the storm's intensity and a cone of certainty for its path. Over the decades, improvements

in data and historical data have enabled forecasters to provide better warnings and predictions.

This is exactly the same process EMDS would use for strategic readiness data, he said. As historical data accumulates and as more databases are mined, the data EMDS produces becomes more reliable. That allows leaders to make more informed decisions.

Hour-by-hour, the power of EMDS grows as it consumes vast quantities of information—allowing operators to better spot patterns, trends and anomalies.

What emerges from the data can sometimes be surprising, he said.

"Readiness indicators we thought of as being valuable might not be and other indicators might be more valuable predictors than we thought," Saxon said. "The data are not just about telling you what you already know. It's making you aware of what you might not have even asked about before. Things pop to the surface you never realized."

"He added that EMDS can currently answer the "who, what, when and where" questions and over time it will begin to answer the "why and how" questions as well.

The model is constantly updated and adjusted based on past predictions and that gives EMDS an increased ability to forecast readiness at the strategic level, he said. "That's where we're headed, but we're not there just yet."

HUMAN-MACHINE INTERFACE

Human interaction with the system is just as important as the reliability of the system itself, Saxon said.

To that end, the team at EMDS maintains a robust user-testing program, he said, both formally and informally. Feedback about the user experience, both good and bad, informs the EMDS team on decisions going forward and what tweaks are needed now.

Saxon said he is very aware that using information technology can be an intimidating and frustrating experience for people if the system is not "friendly."

The whole point of EMDS, he said, is not technology for technology's sake. Rather, it is a tool leaders can use to get the answers they need. If they are getting those answers in an efficient manner, they will adopt the system as their own, he said.

Saxon admitted that not everyone is onboard yet, but that as more and more Soldiers "discover" that EMDS meets their needs, they will adopt it.

CHALLENGES AHEAD

"The most significant capability we've released since May is our Army Forces Index," Saxon said. "The Forces Index provides EMDS users with a visual portrayal of the planned Army force structure through the end of the 2018 Program Objective Memoranda, or POM."

Saxon said the index highlights the power of EMDS.

"It takes previously difficult to access and understand data and turns it into information that is more easily consumable and utilized. This enhances the end users ability to analyze the information and discover trends.

"One of our biggest challenges is helping people realize the value in easy access and understanding of information that they previously did not have access to."

Almost all of the data available in EMDS is currently available in some other system, but may be inaccessible to the average end-user.

"EMDS simplifies data access, understanding and information discovery allowing the user more time for information analysis," he said. "We think of EMDS similar to Google or Yahoo. A basic query quickly leads to useful information previously unknown to the user."

EMDS is only as good as the databases it pulls from. Databases across the Army are undergoing a monumental change, away from "stovepipe" legacy systems to more modern enterprise resource planning systems, or ERPs, Saxon said. EMDS is evolving to handle the newer ERPs.

ERPs are better at integrating the flow of information across an increasingly sophisticated network than are older systems, which work in a slower, more linear fashion.

Leaders and users today are more technologically savvy than they were a few decades ago, he said. They want a more efficient and sophisticated system to inform their decision making.

Saxon himself has worked for a number of years in the private sector, building interface systems not unlike EMDS. He's been the director of EMDS going on three years as a mobilized Georgia Army National Guard Soldier.

His efforts were rewarded recently when the prestigious technology magazine CIO identified him as "one to watch" among information technology professionals that include IT leaders in Fortune 500 companies.

He said he's honored to receive the recognition but that it's a collaborative team effort that makes EMDS a go-to system now and one to watch in the future.

"As the capabilities evolve, we constantly get asked to utilize our data and visualization capability to paint a different picture for a new end user," Saxon said. "I expect our system to continue to evolve this way as our capabilities grow." ■

Shared IT Architecture Leads to Cost Savings

Reducing the Army's budget by consolidating networks

BY CLAUDETTE ROULO, AMERICAN FORCES PRESS SERVICE

A new architecture-sharing and modernization agreement among the Air Force, the Army and the Defense Information Systems Agency will increase bandwidth and network security and avoid more than $1 billion in future costs.

"As the Defense Department continues to move aggressively towards [the Joint Information Environment [JIE]], this partnership is an important step forward," said Teresa M. Takai, DoD's chief information officer.

Due to force structure changes, the Army was left with excess information technology capacity, said Richard Breakiron, network capacity domain manager for the Army's chief information office. At the same time, the Air Force was seeking to modernize its IT architecture to meet the requirements of the future joint information environment.

By partnering and taking advantage of the Army's upgrade to faster multiprotocol label switching routers and regional security stacks, the Air Force was able to identify about $1.2 billion in cost avoidance.

The Army expects to reduce its IT budget by $785 million between fiscal years 2015 and 2019 by consolidating hundreds of network security stacks into 15 joint regional security stacks, which the Air Force will also use.

"It's great to have strong partners as we move toward JIE," said Gen. William L. Shelton, Air Force Space Command commander. "I especially appreciate the tremendous spirit of cooperation that has emerged between the Army, Air Force and DISA teams."

MPLS routers are an industry-standard technology for speeding and managing network traffic flow.

The upgraded routers will increase the backbone bandwidth to 100 gigabytes per second, said Mike Krieger, the Army's deputy chief information officer. At Army installations, network speeds will rise to 10 gigabytes per second, he said. To put that in perspective, Fort Hood, Texas, currently operates at 650 megabytes per second, Krieger said.

Regional security stacks are designed to improve command and control and situational awareness and are essential to enabling a single security architecture in the joint information environment, said Krieger. The move will tremendously increase the network security posture and reduce costs, he added.

"More and more, we're saying that some of the service-delivery capability can be managed at the enterprise level, greatly improving efficiency, effectiveness and security," Breakiron said. But, he noted, to perform these enterprise functions off of the local installation, the IT backbone must be much more robust, because users are relying on it for much more service capability.

The new, larger-capacity routers will help the Air Force and Army converge their enterprise network backbones and gain cost savings in other areas, he said.

"As we do our investment in MPLS, it now allows us to do not only [Voice over Internet Protocol], it allows us to do unified capabilities and it allows us to put much more of this capability up at the enterprise level," Brig. Gen. Kevin Wooton, Air Force Space Command director of communication, said.

Together, MPLS routers and the regional security stack construct improve performance and security, said Air Force Lt. Gen. Ronnie D. Hawkins Jr., DISA director.

"It creates a network that is fundamentally more defensible and more efficient," Hawkins said. He added that the move is a major step in building the Joint Information Environment architecture.

The Army and DISA plan to implement the joint MPLS transport cloud and JRSS consolidation in fiscal years 2013 and 2014 to support operations in Southwest Asia and the continental United States.

The Air Force and the Army will have access to data from JRSSs that are owned and operated by DISA as a joint capability. Army and Air Force cyber components will continue to execute cyber defense on their networks.

"As we modernize the DoD network, the Army is committed to a joint solution that helps achieve the joint information environment," said Lt. Gen. Susan S. Lawrence, the Army's chief information officer.

Light, Efficient, SURVIVABLE

The Army's ULV research prototype hits the ground running

BY TARDEC COMMUNICATIONS

While no military strategist can predict with absolute certainty the requirements for future ground vehicles, or in what theater they'll be needed, Department of Defense scientists, researchers and engineers are getting the wheels of technology in motion today.

At TARDEC, a select group of experts is looking at how to design Army vehicles that can undertake missions across a full spectrum of operational challenges while keeping occupants safe and using fuel efficiently. Leading the pack of Army demonstrator vehicles is the ultra light vehicle research prototype, known as ULV.

Funded by the Office of the Secretary of Defense, the ULV project began with a goal to design, develop and build three identical lightweight tactical research prototype vehicles, emphasizing occupant survivability while also meeting four challenging research objectives:

- Payload – 4,500 pounds.
- Performance – at 14,000 pounds curb vehicle weight.
- Protection – comparable to the mine-resistant ambush-protected family of vehicles.
- Price – $250,000 each in a 5,000-unit production run.

TARDEC's Ground System Survivability group partnered with non-traditional defense contractors to bring their combined engineering expertise to the project.

"While existing military vehicle platforms attempt to balance payload, performance and protection, typical trade-offs result in platforms where survivability concerns have driven gross vehicle weights upward, with negative effects on mobility and transportability," stated Mike Karaki, TARDEC GSS team leader/program manager, ULV research prototype. "Developing a single vehicle that meets survivability, mobility and transportability criteria simultaneously—while maintaining affordability—has remained a DoD challenge."

EFFICIENT ENERGY IS MISSION CRITICAL

As the Army steps up efforts to use energy more efficiently, protect Soldiers, conserve resources and enhance mission capabilities, the ULV project could not have come at a better time.

Assistant Secretary of the Army for Installations, Energy and Environment Katherine Hammack, speaking recently at George Washington

University Law School, stated that an estimated 20 percent of all casualties in Afghanistan occur during logistics and fuel resupply missions.

"Right now, one in every 46 convoys in Afghanistan suffers a casualty," she stated.

When the Army conserves energy resources, it sends fewer resupply missions out and, as a result, Soldiers can stay focused on operations instead of resupply, and crucial assets can be deployed elsewhere.

"Technology and new techniques can work to make you more mission-effective," Hammack continued. "It is a high priority to the Army to become less resource dependent, to increase our mission capabilities and increase our agility."

Based on Powertrain System Analysis Toolkit model predictions, the ULV anticipates a combined fuel economy of 14.7 PTM (payload-ton mpg), or 6.86 mpg, on gravel and paved terrains at gross vehicle weight plus an up-armored kit.

An occupant centric interior provides state-of-the-art protection through a variety of blast mitigating technologies and crew accommodating features including adjustable seats that stroke downward on impact, five-point restraint systems and a spatial layout that helps avoid head impact and flail injuries.

Tests and evaluations are planned through early fiscal 2014 where model predications can be validated and areas for improvement can be analyzed. T&Es on three ULV test articles includes human factors engineering, mobility, durability and survivability tests. Test sites include Aberdeen Test Center, Nevada Automotive Test Center and TARDEC's Ground System Power and Energy Lab. The array of test data from the three test sites will provide a solid understanding of the vehicle's capabilities, limitations and opportunities for development.

ULV BACK STORY

In early 2010, OSD, with support from DARPA, engaged TARDEC to be the executive agent for the ULV research prototype initiative.

The ULV project presents a high-risk, high-reward scenario. And since the program has moved at an accelerated pace—only 16 months from design to prototype—a process using commercial-off-the-shelf technologies, with room for new and innovative developments, were employed.

"OSD was interested in exploring new 'out-of-the-box' and 'outside-the-mainstream' ideas as well as partnering with non-traditional defense partners to rapidly develop a lightweight tactical concept vehicle focusing on four primary research objectives [payload, performance, protection and price] while emphasizing occupant-centric survivability," said TARDEC GSS Associate Director Steven Knott.

"The effort was to investigate the research and development of lighter-weight armor solutions and leverage DARPA-developed vehicular structural technologies. Additionally, the effort would seek to integrate other new, innovative, weight-reducing technologies such as a lightweight diesel engine, hybrid-electric drive, lightweight wheels and tires, and improved long-stroke suspension," Knott said.

The plan called for TARDEC to develop one ULV systems integration platform and three ULV test articles for automotive and survivability testing and evaluation. "The approach would aim to create synergistic survivability, such that these technologies integrated together would produce a result that is greater than with any of the technologies independently," Knott stated. "Soft deliverables such as data and lessons learned, and hard deliverables such as test assets and spare automotive components, will help shape, inform and support tactical vehicle programs, technology demonstrator efforts and/or TARDEC innovation projects to maximize the overall return on investment."

FINAL DESIGN

"An ambitious primary contractor, together with support from TARDEC leaders and the overall ULV team's communication plan, significantly contributed to achieving the rapid design, development, fabrication and integration of the prototype vehicles," Karaki noted.

"Specifically, the contributions of the TARDEC-established integrated product team [IPT], populated by stakeholders and subject-matter experts from various programmatic and technical DoD organizations, supported the contractor's design decisions early and often during the fast-paced effort. IPT feedback combined with modeling and simulation [M&S] and virtual/physical Soldier design reviews also contributed to the ULV's overall design," he continued.

The ULV's final design includes a relatively spacious, contractor (Hardwire LLC)-designed crew-accommodating cab that provides increased interior space than similarly equipped tactical vehicles. The remote-mounted and remote-controlled vehicle electronics reduce HVAC workloads and create significant occupant spatial accommodations.

DOORS AND CAB

The "clam shell" style front and rear doors open away from the B-pillar, creating a protected area for the crew to exit, explained Vladimir Gendlin, TARDEC GSS, Ballistic Protection Lead, ULV Research Prototype. "The doors use over-swing straps to set a maximum open position, along with an insulating foam liner to contribute to thermal stability of crew compartment and HVAC requirements, as well as reducing exterior noise," Gendlin stated. Large windows allow maximum viewing angles and the design accommodates optional add-on armor packages for protection against larger threats.

"The cab is designed to have seven egress points facilitated by quick-release and removable components, stowage space for personal or mission-specific items, and 360-degree situational awareness through front- and rear-mounted ultra wide-angle thermal imagers," Gendlin remarked.

SURVIVABILITY AND BALLISTIC PROTECTION

"Survivability designs include a variety of interior and exterior blast-mitigating technologies to protect its occupants against underbody threats," stated Venkatesh Babu, TARDEC Ground System Engineering Assessment and Assurance-Energetic Effects and Crew Safety, Blast M&S Lead, ULV Research Prototype. "The ULV's hybrid design allows for a 'clean underbody' through the elimination of traditional components such as a driveshaft, transmission, transfer case, and frame rails, potentially allowing for blast mitigation technologies to perform uninhibited during a blast event. This design provides added opportunities to integrate various blast-mitigating kits under the hull for higher threat levels."

For example, interior technologies include a crushable floating floor system that decouples the crew's feet and legs from the steel hull and absorbs energy, adjustable seats that stroke downward on impact, five-point restraint systems, and spatial accommodations to mitigate head impacts and flail injuries. And exterior technologies include a single-piece monocoque crew cab, double "V" pontoons with integrated stiffeners, and rigid structural stiffening technologies.

The vehicle structure is made up of high-strength steels and advanced composite materials offering lightweight ballistic protection from a number of threats while keeping the vehicle's overall weight down.

"With the optional add-on armor package against larger-threat protection," Gendlin remarked, "the ULV utilizes a newly developed transparent ceramic armor system that offers considerable weight reduction and increased visibility as well as a lightweight gunner protection kit and sling harness comprised of advanced composites offering protection to the weapon operator from a number of threats, to include small arms, blast and crash events."

POWERTRAIN

The ULV's hybrid powertrain strives to improve mobility and survivability. "The hybrid drive system eliminates the need for a driveshaft, potentially improving underbody blast performance, as well as providing drive redundancy by way of two electric drive motors," explained Daniel Connell, a contractor who supports TARDEC GSS Test and Evaluation/Systems Engineering, ULV Research Prototype. "This technology, coupled with a lightweight diesel engine, endows the ULV with numerous capabilities, such as immediate electric launch, stealth drive, silent watch, exportable power generation, high torque at low/near zero speeds and likely improved fuel economy," he said.

SUSPENSION

The ULV's lightweight, intelligent, adjustable suspension system (18 inches of vertical travel), provides automatic ride-height adjustments and can be lowered to meet a variety of stowage heights. This system uses silicon-based fluids to adapt the vehicle's response to road and terrain variations and driving styles by automatically and instantaneously adjusting spring stiffness and damping at each wheel, independently, to increase roll/pitch control and stability and reduce ride harshness without driver intervention.

C4ISR

The ULV features lower-weight command, control, communications, computers, intelligence, surveillance and reconnaissance technologies with full Internet Protocol control options, improved integration, with a focus on warfighter needs. According to Karaki, the ULV electronics package represents a full electronic suite capability that exists in comparable tactical vehicles. "The use of a common integrated user interface for radio, shot detection, video and global satellite positioning results in significant space and weight savings. The co-location of the C4ISR components also reduces internal temperatures as well as secondary projectiles in the event of a threat penetration." ■

HEaDS-UP

Helmet electronics and enhanced protection at Natick for better helmets

BY BOB REINERT, USAG-NATICK PUBLIC AFFAIRS

In their quest for better helmet technologies to keep Soldiers and Marines safe on the battlefield, researchers at NSRDEC are making a HEaDS-UP play.

Helmet Electronics and Display System-Upgradeable Protection, or HEaDS-UP, has been a four-year effort at Natick, Mass., to provide mounted and dismounted troops with a more fully integrated headgear system. HEaDS-UP has focused on developing a technical data package of design options and tradeoffs to build a modular, integrated headgear system. Some of these technologies include: improved ballistic materials; non-ballistic impact liner materials and designs; see-through and projected heads-up display technologies; better eye, face and hearing protection; and communications.

Two modular headgear concept designs emerged from the process. They will be officially unveiled in October during a demonstration at Fort Benning's (Ga.) Maneuver Battle Lab, said Don Lee, project engineer in the Headgear Thrust Area of Natick Soldier Research, Development and Engineering Center, or NSRDEC.

"We'll have mounted and dismounted Soldiers wear the two different concepts, performing a variety of tasks," Lee said. "The event

The new integrated helmet technology would eliminate the need for crewmembers to switch to their Army Combat Helmets when dismounting from their vehicles.

will be a VIP demo of Soldiers conducting training operations at mission speed using the helmet concepts."

According to Lee, the advances resulted from the collaboration between NSRDEC and ARL. Quarterly meetings kept dozens of involved personnel on the same page.

"The program was very successful due to the collaborative support from the different agencies," Lee said. "Without that collaboration and support, it would have made the program more challenging."

Lee said that the program looked at a variety of technologies.

"It was mostly like an 80-20 split—80 percent material solution, 20 percent impact on the Soldier," said Lee, "kind of setting the stage for the next evolution of headgear protection, which will look to swap that, doing more 80 percent impact on the Soldier and 20 percent material solution."

The modular prototypes were designed to allow warfighters to adapt the headgear to the mission and to work harmoniously "with other existing, fielded technologies—your body armor, your [hydration pack], your protective eyewear, and then being able to accomplish common skills and tasks—getting up, getting in a prone position, entering a vehicle, exiting the vehicle, sighting a weapon, and stuff like that," Lee said. "We've done some cognitive studies, as well, looking at head-mounted displays, see-through displays, the integration factor of the display."

Mounted and dismounted Soldiers have already worn the prototypes in "human factors evaluations," from which data were collected, analyzed and applied.

"We were able to integrate the concepts during their normal training scenarios, and then following their training event, get feedback from them," Lee said. "It was quite overwhelming, the response [we] received that every Soldier that used these systems liked the prototype systems over their currently fielded system. So whether it was an [Army Combat Helmet] or a [Combat Vehicle Crewman helmet], they all like the prototypes over them."

Lee predicted that Soldiers will embrace the modular platform, from which parts can be added or removed in seconds.

"Being able to don that [mandible and visor] protection when needed or being able to remove it when not needed is the big 'wow' factor," he added.

The mandible and visor provide fragmentation protection for the face, Lee said.

"Going by a recent [Joint Trauma Analysis and Prevention of Injury in Combat] report, of all the injuries to the head, 72 percent are to the face," Lee said. "So that shows a technology gap there.

"Soldiers wear the [ballistic] eyewear, but everything outside the eyewear is open. This will be the biggest advantage to the Soldier." Vehicle crewmembers, in particular, should appreciate the headgear.

"One of the things I hoped to do with this program was reduce the logistic footprint of combat helmets for ground Soldiers," Lee said. "Right now, mounted Soldiers have two helmets. They have their Combat Vehicle Crewman helmet and they have their Advanced Combat Helmet. So, if they dismount from the vehicle, they're supposed to swap helmets.

"I think we've proven through our program that there can be one helmet for both mounted and dismounted Soldiers, which, I think, is a big deal. I think the program's proven that a one-helmet system for ground Soldiers, whether they're mounted or dismounted, can exist."

The Helmet and Electronics and Display System-Upgradeable Protection, or HeADS-UP program, at Natick Soldier Research, Development and Engineering Center, Mass., seeks to provide better headgear for Soldiers and Marines.

Crewmembers looking out hatches discovered an unexpected benefit during evaluations.

"When the Soldiers wore the prototype systems with the visor and mandible," said Lee, "it was the first time that they weren't eating sand and dust and rocks going down the road."

Ultimately, the program data will be transferred to Program Executive Office Soldier and the Marine Corps for decisions about what technologies should be fielded.

"We've come up with tradeoffs, ideas, designs that the Soldier will benefit from in the end," Lee said. "When these technologies impact the Soldier in a positive way, that's really the reward at the end of the day." ■

STEM Outreach

The Army bolsters national cybersecurity through STEM outreach

BY DAN LAFONTAINE, RDECOM PUBLIC AFFAIRS

Computer networks face persistent cyber threats from the nation's adversaries. The future defenders of cyberspace, America's students, honed their skills this summer as they learned from U.S. Army scientists and engineers who are experts in the field.

Cybersecurity practitioners from across the RDECOM joined forces to spark an interest and share their knowledge with high-school students as part of the Army Educational Outreach Program (AEOP) at APG.

Two RDECOM organizations—ARL and the CERDEC—partnered to develop and deliver two Gains in the Education of Mathematics and Sciences (GEMS) cyber programs in July.

Dr. Lisa Marvel, an ARL electronics engineer and one of the program's instructors, emphasized that educational outreach efforts are a priority because of America's growing demand for a robust cyber workforce.

"We should do this for our nation. We may not have enough computer professionals by 2018," Marvel said. "We need a diverse pool. We don't just need the same group of people solving the same problems.

"You need creative solutions to our future problems. You get that through diversity. The more people we can impact in a positive way, the better off we'll all be."

ARL and CERDEC each presented one week of instruction for the cyber GEMS program, allowing for each organization to leverage its specific expertise. The collaboration included the Army Communications-Electronics Command, also at APG, which worked with CERDEC to design its curriculum.

APG is one of 12 GEMS sites for the Army. GEMS is an element of the AEOP portfolio of programs, for which RDECOM provides the oversight.

Erica Bertoli, CERDEC educational outreach program lead, said the science, technology, engineering and mathematics, or STEM, initiatives through AEOP provide students with direct access to Army experts.

"GEMS is unique in that the instruction is led by engineers and scientists currently working in our labs. This not only creates an opportunity for students to access the latest practical information, but it also lets them network with individuals working in the field, to ask questions and get real-world answers," Bertoli said.

Stephen Raio, a CERDEC information assurance engineer and a GEMS instructor, explained that cybersecurity works well as a STEM subject because of its widespread relevance to everyday life. Computer networks touch nearly every aspect of America.

"Networks and computing equipment form the backbone of our country's infrastructure," Raio said. "Our water, power, sewage, telecommunications and food-supply chains all rely on information technology. Cybersecurity is critical to keeping everything running smoothly.

"Cybersecurity is a never-ending arms race, and the goal is to minimize your risk to the best of your ability," Raio explained. "One of the best ways to do this is through defense in depth. Just like a castle has several layers of defense, so must our information technology systems."

CERDEC's course included sessions on basic networking, network protocols, client/server programming, firewalls, digital forensics, cyber attacks and mobile-device security. In addition to cyber, CERDEC also offered an alternative energy GEMS course.

The GEMS instructors stressed that they aimed to keep the course interesting and stimulating through hands-on activities. Lectures were out, and keeping students engaged was in.

"Our main goal was to build confidence and stimulate excitement," Marvel said. "You can do this. It's accessible. We don't come in and say, 'You can't touch this.' Let's take a computer apart. Don't worry about breaking it."

Because the Army scientists and engineers are with the students for just one week, developing a long-lasting passion for computing was the GEMS session's primary goal.

"I would like them to develop a curiosity in computing. I had a parent tell me that her son, who attended our GEMS, came home and said, 'You know that old computer we have? I think I can fix it.' That's a win," Marvel said. "She gave him a screwdriver, and he took it apart. He said, 'I need to go to the store and get new parts.' The parent said he never would have done that before this."

After a student gains an initial passion for computing, having good computer-science teachers in high school and college is vital to growing that interest, Marvel said. The Army hired a local high-school computer-science teacher for the two-week GEMS in an effort to strengthen the connections between practicing computer experts and educators.

"We're trying to further the computer-science education field so that more students choose computing as a field, and we can have a pool of future scientists for the Army," Marvel said. "Some people might be leaning toward teaching but also have an affinity for computing. You don't just have to be a scientist in the lab. You can also be a teacher. To get more people into computing, we need good teachers."

STEM outreach efforts exist not only to increase the number of students interested in pursuing science and engineering career fields, but also boost students' passion for their educations in general, said Dr. Sandy Young, a materials engineer and lead for ARL's STEM program at APG.

"We don't assume that every single student is going to be turned on to STEM by attending GEMS. Developing critical thinking is certainly an important point of Army education outreach. You want citizens who know how to make good decisions," Young said.

Environmental Concerns

Picatinny to remove tons of toxins from lethal rounds

BY CASSANDRA MAINIERO, ARDEC PUBLIC AFFAIRS

An enemy convoy transporting a supply of fuel rumbles across the desert floor, an ideal target for armor-piercing incendiary projectiles.

These projectiles are most useful for "after-armor effects," such as an incandescent flash immediately after penetrating a hard target. The resulting plume may be useful for devastating any fuel-storage facilities by igniting the fuel vapors.

The Army uses a formulation called IM-28 that is charged into certain armor-piercing incendiary projectiles, which can be fired from such weapons as the M2, M3 and M85 machine guns.

The problem with the in-service IM-28 is that it contains two harmful chemicals. At Picatinny Arsenal, the ARDEC Pyrotechnics Division is working to develop an alternate formula that is friendlier to the environment.

Picatinny researchers are working to remove the harmful chemicals barium nitrate and potassium perchlorate from the IM-28 baseline mixture and replace them with a chemical known as sodium metaperiodate.

The result is an environmentally safer mixture that remains within the Environmental Protection Agency's regulatory levels for perchlorates (15 parts per billion) as well as those of the state of New Jersey (5 parts per billion).

However, reformulating military devices, such as pyrotechnics, is challenging as chemists aim to develop formulations that not only reduce risk to the environment, but are also safe to handle, manufacture and shows comparable performance to IM-28.

"Addressing all those things at once, it's like trying to hit a silver bullet," said Jesse Sabatini, a formulation chemist at the Pyrotechnic Division.

The push for ecology-friendly devices gained greater impetus after studies indicated that some barium compounds and perchlorates have debilitating effects on the environment, manufacturers and the Soldier.

Perchlorates are ubiquitous in commercial fireworks and airbags. But, research also shows that perchlorates are a teratogen, thyroid disruptor and can interfere with proper thyroid function.

Similarly, chemicals such as barium nitrate are hazards to occupational health and have been linked to bronchoconstrictor effects. In a military environment, the risks can multiply.

After pyrotechnic munitions combust, for instance, the chemical residue can leech into the ground water and air at training sites. When the Soldier is exposed, it negatively affects the Soldiers' health, as well as hampers the ability to train and prepare for combat, which can reduce combat readiness.

"It's not only important to face the problems of today, but it's also important to face the problem five or 10 years down the road," Sabatini said.

The idea to create perchlorate-free munitions has been of interest since the late '90s, when researchers developed perchlorate-free simulators, such as the flash bang which is a non-lethal device that produces a loud report useful for training or riot control.

But, it wasn't until Jared Moretti, a formulation chemist, arrived at Picatinny that the ideas of replacing barium nitrate and perchlorate with sodium metaperiodate gained traction.

"It [sodium metaperiodate] was a chemical I routinely used as a graduate student for a different application. So, we tried it," explained Moretti, who earned his doctoral degree in organic chemistry from the University of Pittsburgh, in 2010.

Working with the Naval Service Warfare Center at Crane and Alliant TechSystems, known as ATK, the Pyrotechnic Division tested a range of formulations that varied in composition.

Each composition had defined increments of chemicals and contained no perchlorates or barium.

Observing how sensitive each mixture was to impact, friction and electrostatic discharge (the flow of electricity between two objects), results showed that two main oxidizers worked best in the compositions: strontium nitrate and sodium metaperiodate.

These two formulations were then sent to ATK, where manufacturers blended the mixture and charged it into bullets, testing it for incendiary flash and penetration. Testing showed was that one formulation with sodium metaperiodate approached the function test scores of IM-28 and was also brighter.

Testing took more than a year and the new oxidizer has now found widespread application in many ongoing research programs in energetic materials. Incendiary rounds and illuminant signals, are just some examples of product improvement programs that have exploited the new oxidizer.

"When the chemical is implemented into the full device, its test scores are comparable to the in-service IM-28," explained Moretti. "We have very good reason to believe that we can tweak the manufacturing parameter like charge weight—the amount of powder in each bullet—to further improve performance."

Still, being ecology-friendly isn't the only advantage to the reformulation.

Due to the fact that the mixture only requires two chemicals, manufacturers are able to drastically streamline the formulation process from the IM-28, cutting down on production time.

On the other hand, cost varies depending on the availability of the material. While sodium metaperiodate is currently more expensive than perchlorates or barium, Sabatini believes supply and demand will change this.

"You have to look at the total life cycle of an item that is being produced," said Sabatini. "Even though perchlorates are cheaper to manufacture today, regulatory pressures associated with the production, remediation and disposal of the material will drastically increase life-cycle costs."

Instead, the reoccurring issue that Sabatini and Moretti often find themselves against is simpler: obtaining supplies.

Early in testing, for example, the Pyrotechnics Division developed a formulation that required the use of coated aluminum powder, a chemical whose coating makes it reactive. However, given the short supply, the ability to obtain coated aluminum is often a struggle.

Sabatini and Moretti avoided this issue by eliminating the need for coated aluminum powder altogether.

Future steps for the reformulation of the IM-28 include tests to qualify the formula and performance tests for the applications, a process scheduled to occur throughout 2014. ■

Army Using Latest 3D Advancements

The Army is using some of the latest advancements in the areas of composite structures and 3D printing to better equip today's Soldiers.

In particular, engineers at the U.S. Army Aviation and Missile Research, Development and Engineering Center Weapons Development and Integration Directorate incorporate composite technology and additive manufacturing, sometimes called 3D printing, into a solution for Soldiers using the Javelin missile and the Javelin command launch unit.

In anticipation of the future need to integrate Javelin into the network of sensor-shooter systems, WDI proposed a far target locator to provide accurate target data that could be passed from the Javelin gunner to other systems on the network.

But this solution resulted in another problem: added weight.

"If we're trying to reduce their burden, we don't want to give them a system that's heavy, and traditionally these accurate inertial navigation systems are 10 pounds by themselves," said Virginia Franco, a mechanical engineer who worked on the far target locator design.

It was imperative that the far target locator be lightweight. A vendor was found to make lighter weight components for the inertial navigation system, but housing it in aluminum, which is the material traditionally used, was still going to result in too much weight.

So the solution was to bring in the expertise of the AMRDEC Composite Structures Lab team and AMRDEC engineer Keith Roberts, to design and fabricate housing for the FTL using advanced composite materials.

The collaboration on the Javelin FTL is part of the close combat missile modernization technology program managed by Devin Chamness from WDI and is the outgrowth of complimentary component-based development efforts researchers were performing under the Applied Smaller Lighter Cheaper Munition Components program that ended in fiscal 2012.

Army Chemical Lab Develops Mobile Capability

The Field Deployable Hydrolysis System, or FDHS, is a transportable, high throughput neutralization system designed to convert chemical warfare materiel into compounds not usable as weapons.

The FDHS furthers the DoD's mission of chemical agent disposal operations and can be used to neutralize bulk amounts of known chemical warfare agents and their precursors. Neutralization is facilitated through chemical reactions involving reagents that are mixed and heated to optimize throughput with a destruction efficiency of 99.9 percent.

ECBC, in partnership with the Defense Threat Reduction Agency, signed a technology transfer agreement with the Joint Program Executive Office-Chemical Biological Defense, June 27, at Aberdeen Proving Ground, Md.

The official transition took place upon completion of an FDHS operational demonstration for DoD stakeholders, and signified a transition for advanced development and future integration into the Chemical Biological Defense Program Portfolio.

The FDHS is designed for worldwide deployment with operational capability within 10 days of arriving on site location. A 20-week design and development phase was funded by DTRA in February 2013 and ECBC subject matter experts led the effort to construct a functional FDHS prototype with partnering organization, the Chemical Materials Activity.

More than 50 ECBC employees accounted for 13,000 hours of work in order to meet the objective to produce an operational model in six months that could be transitioned from technology development into an advanced development program.

ECBC's life cycle capabilities enabled the chemical-biological defense community to maintain pace with the emerging requirements of the operational environment. The center's rapid prototyping capabilities and field operational experience were vital to the design and functionality of the FDHS. Engineers and technicians discussed various design plans and 3D models, and screened and analyzed commercially availabl e technologies throughout the process. ECBC's technical expertise was combined with CMA's experience in building and operating chemical agent neutralization facilities that have safely and successfully completed their chemical agent disposal missions.

Read more: http://1.usa.gov/19EPEsY

Latest Version of America's Army Ready for Download

The next version of the America's Army video game was recently released and is now available for download.

Players can register their Soldier name for the game at the America's Army: Proving Ground website, www.americasarmy.com, and then jump into the Army action.

America's Army is developed out of the Software Engineering Directorate of the U.S. Army Research, Development and Engineering Command's Aviation and Missile Research Development and Engineering Center at Redstone Arsenal. While more than a decade old, the game stays new and relevant with frequent updates and new product lines.

This newest version emphasizes small unit tactical maneuvers and training that reflects the current day Army and emphasizes Army Values, teamwork, training and completing the objectives through gameplay that reflects the Soldier's Creed.

"We took a back to basics approach that highlights a move, shoot, communicate system within a fun gaming experience that echoes teamwork-based Army training," said Marsha Berry, Project Manager for America's Army. "Just like in the Army, America's Army: Proving Grounds focuses on creating elite, well-trained Soldiers that will complete the missions as a fine-tuned team beginning with smaller, focused exercises and advancing up to larger, more complex exercises."

Highlights of the latest offering include fast-paced Battledrill Exercises for small engagements of 6-on-6 play; Forward Line Operation training for 12-on-12 play; new weapons such as the M9 and Remington 870 MCS shotgun and M14EBR-RI sniper rifle; and self aid where players can stabilize themselves and get back into the battle quicker.

Set in a fictional country, The Republic of the Ostregals, players are in the role of an 11B Infantryman practicing combat maneuvers at Joint Training Center, or JTC, Griffin, a fabricated training military operations on urban terrain, or MOUT, environment created by Conex modular containers and found materials.

The America's Army Comics series at http://comics.americasarmy.com/ unveils the storyline that influences the plot for the game's missions and maps and gives the player a better understanding of their assignment and the challenges they will face. By reading the comics, players learn the saga of American forces deployed to Czervenia, a tiny foreign nation in the middle of a chaotic conflict. From a seemingly insignificant nation of Czervenia, President-General Adzic and his army set upon a campaign of annihilation against the neighboring Republic of the Ostregals, setting in motion a mysterious plan that could change the course of world power forever. America's Army must create new experimental combat teams, forged together in secret proving grounds, and uncover the general's insidious plot before time runs out.

http://www.army.mil/article/110319

West Pointers Visit Picatinny

Jim Zunino, an ARDEC materials engineer who works at Picatinny Arsenal, showed U.S. Military Academy cadets an ink-jet printer munitions antenna. The antenna utilizes silver nanoparticles printed onto a flexible polyimide substrate.

The visiting cadets were students in one of the Academy's chemistry classes who visited several ARDEC energetic laboratories at Picatinny September 9-10. During the tour, the cadets learned about applications of chemistry and its potential military uses. They also learned about research and development work being conducted at ARDEC in support of the Army.

West Point cadets have been conducting the educational tour since 2010, although it was cancelled last year because of Superstorm Sandy.

TARDEC Leaders Engage with Partners

Leaders from the U.S. Army Tank Automotive Research, Development and Engineering Center strengthened connections and laid the groundwork for new collaboration at the ground vehicle community's preeminent event to drive strategies for the development and support of cutting-edge, break-through technologies.

At the National Defense Industrial Association Michigan Chapter's 5th Annual Ground Vehicle Systems Engineering and Technology Symposium, or GVSETS, and the TACOM Life Cycle Management Command (LCMC) Plans & Priorities Symposium, government and industry stakeholders discussed the latest in ground vehicle technology and how to plan the pathway forward in today's fiscal environment.

Decreasing budgets are pressing government agencies and defense contractors to rely more on partnerships and to find innovative ways to deliver cost-effective technological improvements for the military.

"It's more important than ever that we're transparent with what we know and what we think we know," said Kevin Fahey, program executive officer for PEO Combat Support and Combat Service Support. "This event allows us to ask important questions such as what capabilities do we have today, what technology do we need to go forward and what are our resources?"

The eight main topics presented at GVSETS included: Operating in the New Defense Environment; Technology Transition; Technology Applications/Opportunities for Ground Vehicles; Impacts of the Current Defense Environment on Original Equipment Manufacturers; Systems Engineering Education and Collaboration; Impact of Sequestration and Continuing Resolution; Integrated Logistics Support/ Sustainment; Long-Range Ground Vehicle Science and Technology Strategy.

U.S. Army Tank Automotive Research, Development and Engineering Center, known as TARDEC, Director Dr. Paul Rogers unveiled the organization's long-range strategy during a panel discussion with TARDEC Executive Directors Magid Athnasios, Systems Integration and Engineering; and Jennifer Hitchcock, Research and Technology Integration; along with Dr. David Gorsich, chief scientist.

"TARDEC invites the collaboration that makes our forces so dominate the adversary knows the battle is lost before it starts," Rogers said.

The main session culminated with a Warfighter Panel—a discussion featuring active duty service members recently deployed to Iraq and Afghanistan.

"Soldiers have to trust your equipment to use it," explained Sgt. Maj. Eric Volk, 7th Infantry Division. "Without trust, equipment will sit in the corner and it won't get used."

A new addition to GVSETS was the TACOM LCMC Plans & Priorities Mini-Symposium, in which ground system leaders laid out road maps for industry opportunities, technology development and modernization. This addition to the symposium provided a great opportunity for information sharing to help the program executive offices, TARDEC, industry and academic partners align future technology investments.

With more than 700 people in attendance, GVSETS continues to help cultivate and preserve the kind of collaboration among stakeholders that make ground vehicle developments successful.

"Maintaining the tactical edge helps keep us the best military in the world," Volk reminded the GVSETS attendees. "We put our trust in you."

Best Papers

Aided by the Internet, Dr. Kevin Chan, electronics engineer, and Dr. Jin-Hee Cho, computer scientist, of ARL's Computational and Information Sciences Directorate's Tactical Network Assurance Branch, were recently recognized with the Best Paper Award at the 22nd Annual Conference on Behavior Representation in Modeling and Simulation, or BRiMS, held at Carleton University in Ottawa, Canada.

The BRiMS conference enables modeling and simulation research scientists, engineers and technical communities across disciplines to meet, share ideas, identify capability gaps, discuss cutting-edge research directions, highlight promising technologies and showcase the state-of-the-art in applications.

Papers presented at this year's BRiMS conference analyzed human factors and human-machine systems through modeling and simulation of empirical data related to areas including modeling and simulation in military domains, tools for building distributed/ large-scale M&S systems, data-driven modeling and simulation, virtual world research, biological influences in behavioral models and networked systems models/ social cognition.


IF OUR ACTIVE BLAST MITIGATION
SYSTEM SOUNDS LIKE SCIENCE FICTION.
REMEMBER THERE WAS
A TIME SUBMARINES AND
AIRPLANES DID, TOO.
EVERY ONCE IN A WHILE, something comes along that's so innovative, it changes everything. The world's first ACTIVE underbody blast mitigation system is that kind of breakthrough. One that will dramatically increase the survivability of our troops against IEDs.
A lightweight system that detects and counters the accelerating force of an IED within milliseconds. It's the active blast system everyone's been waiting for. Proven by independent tests, compact, lightweight, universally adaptable, and ready for evaluation and deployment on your platform.
Because there's no such thing as too much protection.
TenCate ABDS™ active blast countermeasure system
TENCATE
materials that make a difference
www.TenCateABDS.com
email: ABDS@TenCate.com

"I will take a look at programs that allow us to keep the best because we need our scientists, we need our engineers, we need our Ph.D.s to help us to come up with the new ideas and technologies to take care of our young men and women in uniform."

—Testimony from Gen. Ray Odierno, Sept. 18, 2013
House Armed Services Committee hearing