

Army researchers looking to blend electronic warfare

By Kristen Kushiyama

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, the U.S. Army Research, Development and Engineering Command's Communications-Electronics Center, known as CERDEC, researches the technologies, standards and architectures to support the 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," said Robb.

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," said Bertoli.

"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," said Bertoli.

The Army professionals find themselves 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," said Bertoli.

"The ability to leverage both cyber and EW capabilities as an integrated system, acting as a force multiplier increasing the



Photo illustration courtesy of the U.S. Army Research, Development and Engineering Command's Communications-Electronics Center

Developers in the U.S. Army Research, Development and Engineering Command's Communications-Electronics Center Integrated Cyber and Electronic Warfare, or ICE, program look to leverage both cyber and Electronic Warfare capabilities as an integrated system to increase the commander's situational awareness. CERDEC leaders are focusing their development efforts on researching solutions to address specific cyber and Electronic Warfare threats and developing the architecture onto which scientists and engineers can rapidly develop and integrate new more capable solutions.

commander's situational awareness of the cyber electromagnetic environment, will improve the commander's ability to achieve desired operational effects," said Robb.

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," said Bertoli. "The Army [leadership] 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," said Bertoli. "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."

(Continued on page 40)

(Continued from page 39)

“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,” said Bertoli.

“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,” said Bertoli.

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,” said COL Dupont.

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,” said Robb.

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,” said Bertoli.

