EDITORIAL WHITEPAPER

C4ISR&NETWORKS
www.C4ISRNET.com

Bridging the interoperability gap

Underwritten by:
REDCOM

Bridging the interoperability gap

Military faces need for interoperable comms at the tactical level

BY ADAM STONE

Advances in technology are helping to break down the barriers to telecommunications interoperability that have long stymied military planners. These advances greatly improve military communications capabilities, providing unprecedented situational awareness, better security and broader options for virtually every communications scenario.

While today's military boasts a range of telecommunications technologies, compatibility issues can arise. Voice over Internet Protocol (VoIP), time-division multiplexing (TDM), satellite communications, cellular, tactical radios, SCIP cryptographic devices, Wi-Fi and WiMAX: All are useful, but they don't always play well together. This can have harmful tactical consequences. In a battlefield scenario, for example, it is unacceptable for the front line to lose contact with the command center.

Recently, solutions have emerged that help to solve the incompatibility problem. Improved interoperability is giving the military a tactical advantage, offering greater assurance that messages will get through.

One successful attack vector involves the evolution of a shared adherence by technology providers to published standards and interfaces. With solutions based on open, nonproprietary standards, the military is increasingly able to configure a seamless communications environment across a range of devices and platforms.

These advances are being greeted warmly by many in military circles. With financial institutions and retail organizations generating secure transactions with seeming ease, "we need to do the same thing every day, to keep people's lives safe," said Cindy Moran, director of network services at the Defense Information Systems Agency (DISA).

BRIDGING THE GAP

The technology exists to carry signals seamlessly between VoIP and TDM networks and to ensure connections among diverse devices. Using it could enable interoperability across the military services as well as among America's allies and coalition partners. It's possible to move voice traffic uninterrupted between headquarters leadership and war fighters in the field. But it rarely happens that way.

Why aren't military communications systems more interoperable, and how can planners go where they need to go? To answer this, it helps to step back and see the military's needs in perspective.

In the coming years, military communications likely will be an amalgam of differing networks including IP, TDM and other legacy or emerging technologies. The military will be faced with the challenge of creating seamless links internally and with its NATO allies and coalition partners in the field and at the command level.

SOME OF THE HURDLES EXIST AT THE HARDWARE LEVEL

"The real interoperability challenges come on the modem side because there are so many variations of protocols that are available. Typically, each vendor wants to add in their own value-added protocols" and each unit in turn wants to acquire a particular set of capabilities, said Walton Brown, product director, satellite terminal systems, Army Program Executive Office Enterprise Information Systems.

"It happens at the tactical level where you have different communities buying modem products that suit their particular architectures. Those communities could be Army WIN-T (Warfighter Information Network-Tactical), the Army combat support community, the global broadcast system," Brown said. "It becomes cumbersome, as each community develops more communications requirements, as they adopt more commercial hardware into their architecture to take advantage of the latest protocols. You end up having to keep on layering additional equipment."

In addition to hardware, network infrastructure can be an impediment. As things stand today, different protocols do not easily communicate with each other. Users of traditional and Internet-based networks, for example, cannot readily connect. As a result, modern war fighters still find themselves divided by these incompatible networks: Those operating in the IP world cannot connect to those in the TDM world, a circumstance that has real operational implications for those on the ground.

"We know of several operations that took place over there where U.S. forces on combat maneuvers wound up talking to coalition forces using Iraqi civilian commercial cellphones. It's

INTEROPERABLE VOICE COMMUNICATIONS

really a worst-case scenario," said Eugene Kohlmeier, director of government technology at REDCOM Laboratories, a Victor, New York-based designer and manufacturer of IP-enabled telecommunications solutions for the military and other industries.

With these ad hoc, off-the-shelf stopgaps, issues of encryption and security rise to the fore. "When we have had U.S. military operations in the vacating war zones of Afghanistan and Iraq, we sometimes wind up with a scenario in which U.S. units are talking on radios with encryption, but the coalition forces do not have the same encryptors, so they could not talk to one another directly," Kohlmeier said.

Today's cobbled-together solutions are insufficient. "A lot of times you will have U.S. providing the capability just to make sure we can achieve that security level," said DISA's Moran. "When we really just cannot solve it any other way, we provide [to coalition partners] our stuff and the people to work our stuff, but that is not the preferred method."

> 'We know of several operations that took place over there where U.S. forces on combat maneuvers wound up talking to coalition forces using Iraqi civilian commercial cellphones.
>
> **Eugene Kohlmeier, director of government technology at REDCOM Laboratories**

THE NEED FOR SPEED

Connectivity across standards and devices is an urgent necessity. Without seamless communications, troops and military leaders alike may find themselves lacking the crucial situational awareness capabilities they need to get the job done safely and effectively. Communications exist toward an end, after all: the sharing of vital information. Without good information, a dangerous situation becomes more dangerous.

Yet telecommunications stovepipes still predominate in many parts of the military, in part due to an acquisitions process that ties up users in rapidly aging technologies. Given the nature of long-term contracts, the government may get encumbered in technology that is five or more years out of date. That lag time in turn leaves a gap in interoperability. In some cases, for example, the contracts tie government to inefficient networks such as the Integrated Services Digital Network (ISDN), a standard already dismissed by the vast majority of users and providers on the civilian side.

Satellite communications likewise can falter as the downlink signal is switched into different terrestrial networks. "Some of the applications require more bandwidth and less latency," Moran said. Pair a bandwidth-hungry application (such as voice) with a network of inadequate bandwidth, and the result is not communication, but an unintelligible stream of noise.

In an effort to work around connectivity issues, end users may be making undocumented changes to their equipment in order to get to needed functionality, thus further hampering efforts toward seamless intercommunications.

SECURITY: THE LONG-STANDING ISSUE

In practical terms, the communications breakdown today typically is due to the method of carrying calls. ISDN lines do not have nearly the voice, data and video capabilities of today's IP-based systems, nor can the two readily interconnect. Yet much of the military remains locked into the older methodology. Even as VoIP continues to rise in prominence, the military still lags behind in the use of it. Even as intelligence has migrated to end terminals in the IP world, the continued use of legacy networks hinders military leaders from taking full advantage of these capabilities.

The Pentagon has signaled that it wants these problems addressed in the near future, with leadership calling for a more unified set of capabilities by 2016. This would include the ability to share voice, video and data on a single network. Such convergence would streamline costs and enable enhanced coordination, with interoperable calling serving as a key piece of the puzzle.

Thus far it has been challenging for end users to place point-to-point calls in today's segregated environment – especially given the added layer of complication that comes with the need for military-grade security. If networks were freely conjoined and traffic flowed openly without concerns for security, interoperability would likely be less of an issue. But security concerns preempt such a possibility. Military communications traffic must be locked down tight, with different levels of security for different levels of communication.

Planners have often, and quite rightly, put rigid controls over the security of voice and data flow. As a result, however, the rigidity of the structure has in fact hindered the ready sharing of communications across platforms. These necessary security controls sometimes have effectively shut off the possibility of connectivity between disparate systems. "They have built a moat, which is good, but now they don't know how to get across the water," as one analyst put it.

INTEROPERABLE VOICE COMMUNICATIONS

NEW SOLUTIONS

Despite these diverse hurdles, interoperable communications are increasingly becoming a reality in military circles. Solutions based on published standards and interfaces are helping to take down the walls, creating seamless communications networks that operate across a range of devices and platforms.

One example comes from REDCOM. Certified as a DISA Local Session Controller, REDCOM's solutions cut across virtually all media, moving communications through data networks, conventional voice, satellite and radio, thanks to a philosophical and practical commitment to published (open) standards.

For military telecommunications planners looking for interoperability, REDCOM's efforts may give a hint as to possible solutions. Specifically, the company has hung its hat on a commitment to support a spectrum of open standards including SIP, SCIP, V.150.1, T.38, IPv4, IPv6, ANSI 619a, MLPP, Q.955, C7, SS7, GR-303, V5.2, CAS, DTMF, MFC/R2, MF/R1, FGC, CLASS, ISDN, PRI/BRI and Euro ISDN.

This ability to interoperate even with legacy systems can be a significant advantage to military network planners, as it allows them to utilize existing legacy resources within their communications plans.

"You need to carry forward the technology from the legacy world and add together all these other capabilities within a single box. It becomes an issue of transportability; it becomes an issue for the individual who is doing installation and maintenance, who needs something scalable, something small and deployable," Kohlmeier said.

On a conceptual level, for any solution to deliver true interoperability, there needs to be some interplay between hardware and software components. "There needs to be the hardware interface with the signaling layer itself, combined with software to interpret the varied protocols. The software should be developed to allow this interoperability, including the applications that allow you to send the varied signals and to convert those into interoperable operations," Kohlmeier said. "You need hardware that can connect directly to their system and the software that can connect to the protocol they are using."

If REDCOM's experience is typical of industry advances, adherence to published standards may well be the key to secure and interoperable C2 communications going forward.

What remains to be seen is whether the military will muster the strategic and economic will to pursue such solutions.

"The trouble we have is one of resources," Brown said. "Because we have multiple architectures out there, we do end up having to install duplicate infrastructure. In a world of dwindling resources, we are going to be in a situation where those funds are going to be harder to come by. It's becoming harder to afford all the different community-specific architectures." ■