
Helping Info Flow Freely

Insurgents Outdo U.S. Military, Says U.S. 3-Star

Appeared in Defense News, January 28, 2008

By William Matthews

The U.S. military may have invented network-centric warfare, but in some practical ways, the insurgents in Iraq have mastered it, says a former U.S. commander of U.S. and allied troops in Iraq.

Although U.S. forces have multiple high-speed networks, video teleconferencing, digital mapping, satellites and tons of high-tech gear designed to make battlefield information instantly available to troops who need it, it also has a hierarchical bureaucracy that strives - and too often succeeds - in doing just the opposite.

"Information is firewalled by the bureaucracy," Lt. Gen. Peter Chiarelli told an audience at a network-centric warfare conference Jan. 23. "Commanders are unable to get the information they need because of bureaucratic obstacles."

By contrast, information flows freely among Iraq's insurgents, he said. Although they lack the sophisticated equipment the United States takes to war, they have cell phones, video cameras, Internet access and e-mail. And that's enough to make them highly adaptable foes, he said.

During his tour as commander of multinational forces in Iraq in 2006, Chiarelli fought the U.S. bureaucracy as well as the insurgents.

He's been back in the Pentagon for a year as a senior military assistant to Defense Secretary Robert Gates, but Chiarelli still rails against the "security Nazis," op-sec bureaucrats and overclassification that prevent information from getting to the troops when they need it.

And he expresses something akin to admiration for the speed and simplicity of the insurgents' ad hoc use of networks.

On a 2004 tour in Iraq, Chiarelli led the U.S. Army's 1st Cavalry Division and supported the use of a relatively simple intranet setup so soldiers returning from a patrol could post information that would be useful for those going out on the next patrol. It was called CAVNet after the 1st Cavalry Division.

The idea was to shortcut the traditional information trail, which required incident reports to be passed up through a multilayered chain of command before they could be passed along to the troops on the ground.

A platoon leader couldn't just talk to another platoon leader, Chiarelli said. Incident reports would have to be passed up to the brigade commander and sometimes to the division commander. By the time they were approved for distribution to the next platoon going out on patrol, it was often 48 hours too late, he said.

Soldiers liked CAVNet, but it made security officials nervous. Chiarelli was told his troops could not use CAVNet on NIPRNet, the military's "unclassified but sensitive" network. It could be used only on SIPRNet, the secure network.

Of course, SIPRNet wasn't as widely available as NIPRNet, Chiarelli said, so that security rule undercut the intent of CAVNet, which was to make it easier to get information to frontline troops.

CAVNet and a number of similar military networks are the product of a new generation of troops who grew up with the Internet, said Trey Hodgkins, vice president for defense programs at the Information Technology Association of America.

"They don't come with the cultural inhibitions we have about sharing information," he said. "They're used to it, they see the benefit to it."

And when they are put in an environment that lacks that capability, "they create it," Hodgkins said. "They're pretty easy to create. And they do it outside the normal IT acquisition structure."

"If I had my way," Chiarelli said, every soldier would have a PDA - a hand-held computer linked to a network - to receive information in the field.

Can't do that, security officials said. It would be too easy for information to get to the insurgents.

"It's like when the military doesn't want to talk to the press about a roadside bomb that blew up a Bradley [fighting vehicle] because they don't want the enemy to know how successful he was at blowing it up," Chiarelli said. "He already knows that."

CAVNet was intended to inform U.S. troops of things the insurgents already knew, such as new enemy tactics and procedures, what to watch out for, and what worked and what didn't for U.S. soldiers.

Chiarelli praised another battlefield information innovation, TiGRNet - software that allows soldiers to download intelligence, including digital photos other soldiers have taken, maps, written observations, GPS data and the like.

Like CAVNet, TiGRNet (which stands for Tactical Ground Reporting Network) bypasses the traditional paperwork trail for intelligence gathered on the battlefield. The information goes directly onto TiGRNet rather than being routed first to intelligence analysts.

"It gives the individual soldier the ability to get information quickly," Chiarelli said. "We've got to look for ways to pass knowledge as quickly as possible across the battlefield."

To the hierarchical U.S. military, this is a new and somewhat worrisome concept.

On a PowerPoint slide, Chiarelli depicts the U.S. military as a series of large dots arranged in a pyramid, each dot connected to the dots above and below. Thus, information from one dot at the bottom must flow to the top before it can flow back down to the next dot over.

The Iraqi insurgents are depicted as dots along a line. Each Iraqi dot can communicate with any other dot. It's a flat organization that can pass information very quickly, Chiarelli said. "He can pass information faster than we can. And he uses that information to change the way he fights the fight."

The U.S. military should take heed.

"We need to flatten our information system" and increase the ability of U.S. troops to share information "horizontally," Chiarelli said, meaning that less information should be forced up the chain of command before it is passed on to frontline troops.

[Homepage](#) | [Management Profile](#) | [Sitemap](#) | [Contact Us](#)

©2007-2008 Ascend Intelligence LLC. All rights reserved.