

IT VS. INITIATIVE: THE INTERNET AGE COMES TO THE BATTLEFIELD

By Tyler E. Boudreau

June 25, 2008

On a late summer night of 2004 in al Anbar province, Iraq, just south of Abu Ghraib, an observation post (OP) of four Marines was shot at briefly from the shadows. The Marines made out two silhouettes in the distance, returned fire, and pursued them into the darkness. One of the Marines said to the others as they searched the area, "I think I got one!" But no sign of them was found. Moments later, in a small tent several miles away, I read their report on my computer delivered by email.

Fifteen minutes after that, another report came in over the radio from a different Marine foot patrol in the vicinity. They'd stopped a vehicle and found two men inside; one of them had a gunshot wound to the shoulder. The driver told the Marine patrol leader that his friend had been caught in the crossfire of a civil dispute run amok. He was rushing him to the hospital.

It was a likely enough scenario -- we routinely saw the results of these sorts of incidents -- but the patrol leader quickly called me to be sure. "This guy is bleeding pretty bad," he said. "You want me to let them go? Or do you want to send us a Medevac?" He didn't know about the OP engagement that had taken place less than a mile away.

"Tell him to hold on to them," I said to my radio operator. "I'll have a helicopter there in five minutes." As I spoke, I began generating my own report on my laptop to send up to headquarters.

The entire chain of command knew what was happening even before it was over.

This is the nature of the modern battlefield.

I joined the Marine Corps when I was eighteen. That was in 1989, when the great Soviet armored divisions were still considered our primary threat, Communism was still the prevailing ideology to fear, and infantrymen ("grunts" or "ground-pounders" as we're often called) never ever touched computers.

How times have changed. Modern warfare is predominantly made up of decentralized small-unit actions and low-intensity skirmishes in **complex "semi-permissive" settings**. Today's adversaries are not assembled into the ponderous formations of yesteryear with static defenses and unwieldy supply lines. The prototypical "enemy" of the twenty-first century is an urban guerilla who is mobile, adaptive, and draws his strength and resources primarily from the indigenous population. The prototypical soldier needs more than a rifle to deal with him. He requires a different skill set, and needs speedy communications.

Coming from an older generation of infantrymen, I was astonished to see my unit suddenly being outfitted with every variety of electronic equipment, from "ruggedized" laptop computers with Internet access and instant messaging, to man-packed tracking systems, to a plethora of cameras, videos, and other imagery devices. These innovations were introduced to the battlefield in hopes of increasing situational awareness, rapidly gathering data, analyzing it, organizing it, then pushing it back out to operators as actionable intelligence. They also provide commanders with the freshest possible information and aid them in their moment-to-moment decision-making.

But with the diffuse and often dynamic nature of today's battlefield, the military discovered it needed not only a new line of electronic gadgets, but a new breed of soldier as well -- a thinking soldier.

Commanders can no longer grab their men by the collars of their flak jackets and direct them toward an objective, because in most cases their men are out of reach and the objective is not a point on the map. They depend on their small-unit leaders, who contend with an infinite assortment of situations and variables, to understand the mission, evaluate the circumstances carefully, and exercise initiative in the absence of orders. The military's training has undergone painstaking changes over the past decade to produce exactly this kind of soldier.

Unfortunately, high-speed communications and bold initiative do not always go hand in hand. With such an abundance of information available simultaneously at all levels, micromanagement can creep unnoticed into the chain of command and pull it apart. For example, if a general is able to follow an ongoing firefight through email and IM, and he is inclined to believe he knows what's best for the units in contact, then he very well might start directing those small units from afar, consequently eliminating the need for his colonels, captains, and sergeants to do any thinking of their own.

I witnessed this firsthand in al Anbar. The incidents I described earlier were not so tidily wrapped up, as I'd first assumed. Just as I was explaining my request for a medevac to headquarters, my radio operator informed me that we'd lost contact with our patrol before we could tell them about the OP shooting or get their location for the helicopter. We tried to reestablish comms for twenty minutes, but to no avail. When we finally did reach them, the patrol leader had already made the command decision to let the car go on its way.

Headquarters was furious. It seemed to me that the patrol leader made the humane call given the information available to him; furthermore, we had no actual evidence connecting the two men in the car with the shooting, so I figured we ought to just put the whole thing behind us. But headquarters had no intention of dropping it that easily.

It was as though the whole war was suddenly lost and they had nothing better to do than wring their hands and wonder desperately how the hell we'd ever let those men go. For the next several hours, I was bombarded with emails from headquarters demanding answers. Every question was preceded with the ominous phrase: "The General wants to know . . ."

"Why did they let them go?"

"I've already told you why," I muttered to myself irritably. Then I replied on my computer via email, "Because they didn't know about the OP shooting."

"Why didn't they ask?"

They did ask! I thought as I wrote back, "They did ask. We just didn't answer back in time."

"Why didn't they wait?"

"Because the man was bleeding to death."

"What was the caliber of the gunshot wound?" (They actually asked.)

No idea. I don't think they broke out their tape measures or ripped off the man's bandages. Then I typed angrily, "Unknown."

"How much blood was lost?"

"A lot."

"Why didn't they evacuate the men themselves?"

"Because they were on foot."

"Why didn't they pursue them once you re-established comms?"

"Because they were on foot."

"Which hospital were they going to?"

"Unknown."

"Why didn't they ask?"

"Unknown."

"Why didn't they check out the hospitals and medical clinics in the area? Why didn't they try to find them? Why didn't they do more to get them back? Why did they let them go in the first place?"

By the following morning my head was popping with ire. A million rebukes came to mind. I don't know, I wanted to shout back. Unknown, all right? Because they were on foot, okay? Because they were stupid. Because they were decent human beings. Because they weren't mired in cynicism.

Because they erred on the side of humanity. It was a big fat mistake. They made a call. We can't reverse it. It's over—a shot down-range. We can't get them back. The horse is dead already. Let's just take this opportunity to assume the best. The men were innocent. The patrol leader did the right thing. He saved a life. And let's congratulate him.

But headquarters did not share my optimism and continued its electronic inquiry for two more days until it finally got bored of my increasingly sarcastic responses and stopped writing.

While digital networks have the ability to send, receive, and store infinite amounts of data, there is a natural limit to how much of it any headquarters staff, no matter how robust, can process.

Furthermore, there is a limit to how much a soldier on the ground can convey with the pressures of time, heat, exhaustion, and possibly enemy fire bearing down. Ultimately, the potential of the network falls greatly to the capacity of its end-users. Consequently, any tactical picture formed in remote command posts can't help but obscure the nuances of the peculiar scenarios that patrolling soldiers face on the ground.

The situation is further complicated by the intense political climate of the contemporary battlefield, in which nearly every interaction a soldier has with the local populace, violent or otherwise, can have global repercussions. In such a delicate atmosphere, commanders may grow reluctant to allow their small-unit leaders the freedom to make their own decisions. With the wide array of new communications assets at

their fingertips, commanders can easily develop a habit of micromanaging their troops from afar. Given their inherently limited tactical picture, that is a slippery slope at best.

Even if it is successfully climbed, a commander may be dismayed to find his soldiers have become too heavily reliant on headquarters for critical decisions. That's dangerous, because sooner or later headquarters won't be available. Equipment will break; signals will be lost; communications will go down, and almost certainly at the worst times. That's when the commander will wish most that he had cultivated his men's initiative rather than tamped it out through incessant electronic directives or rebukes for mistaken decisions.

I never did pass on headquarters' harangue to the patrol leader. It seemed to me best not to. The conflicting demands of a commander's need for an independent-minded, mission-oriented soldier and his voracious appetite for information cannot be reconciled by technology. It's a human issue and a leadership issue. Computers will undoubtedly continue to improve and be employed on the battlefield in new and amazing ways; the hardest question for commanders may turn out to be when to shut them off.

<http://www.thestandard.com/news/2008/06/25/it-vs-initiative-internet-age-comes-battlefield?page=0%2C0>