

It takes a network

By Stanley A. McChrystal

*Reprinted with permission from
Foreign Policy Magazine*

From the outset of my command in Afghanistan, two or three times each week, accompanied by a few aides and often my Afghan counterparts, I would leave the International Security Assistance Force head-



GEN (R) Stanley A. McChrystal commanded U.S. Army forces in Iraq and Afghanistan during his career.

quarters in Kabul and travel across Afghanistan -- from critical cities like Kandahar to the most remote outposts in violent border regions. Ideally, we left early, traveling light and small, normally using a combination of helicopters and fixed-wing aircraft, to meet with Afghans and their leaders and to connect with our troops on the ground.

But I was not alone. There were other combatants circling the battlefield. Mirroring our movements, competing with us, were insurgent leaders. Connected to, and often directly dispatched by the Taliban's leadership in Pakistan, they moved through the same areas of Afghanistan. They made shows of public support for Taliban shadow governors, motivated tattered ranks, recruited new troops, distributed funds, reviewed tactics, and updated strategy. And when the sky above became too thick with our drones, their leaders used cell phones and the Internet to issue orders and rally their fighters. They aimed to keep dispersed insurgent cells motivated, strategically wired, and continually informed, all without a rigid -- or targetable -- chain of command.

While a deeply flawed insurgent force in many ways, the Taliban is a uniquely 21st-century threat.

Enjoying the traditional insurgent advantage of living amid a population closely tied to them by history and culture, they also leverage sophisticated technology that connects remote valleys and severe mountains instantaneously -- and allows them to project their message worldwide, unhindered by time or filters. They are both deeply

embedded in Afghanistan's complex society and impressively agile. And just like their allies in al Qaeda, this new Taliban is more network than army, more a community of interest than a corporate structure.

For the U.S. military that I spent my life in, this was not an easy insight to come by. It was only over the course of years, and with considerable frustrations, that we came to understand how the emerging networks of Islamist insurgents and terrorists are fundamentally different from any enemy the United States has previously known or faced.

In bitter, bloody fights in both Afghanistan and Iraq, it became clear to me and to many others that to defeat a networked enemy we had to become a network ourselves. We had to figure out a way to retain our traditional capabilities of professionalism, technology, and, when needed, overwhelming force, while achieving levels of knowledge, speed, precision, and unity of effort that only a network could provide. We needed to orchestrate a nuanced, population-centric campaign that comprised the ability to almost instantaneously swing a devastating hammer blow against an infiltrating insurgent force or wield a deft scalpel to capture or kill an enemy leader.

When I first went to Iraq in October 2003 to command a U.S. Joint Special Operations Task Force that had been tailored down to a relatively small size in the months following the initial invasion, we found a growing threat from multiple sources -- but particularly from al Qaeda in Iraq. We began a review of our enemy, and of ourselves. Nei

ther was easy to understand.

Like all too many military forces in history, we initially saw our enemy as we viewed ourselves. In a small base outside Baghdad, we started to diagram AQI on white dry-erase boards. Composed largely of foreign mujahideen and with an overall allegiance to Osama bin Laden but controlled inside Iraq by the Jordanian Abu Musab al-Zarqawi, AQI was responsible for an extremely violent campaign of attacks on coalition forces, the Iraqi government, and Iraqi Shiites. Its stated aim was to splinter the new Iraq and ultimately establish an Islamic caliphate. By habit, we started mapping the organization in a traditional military structure, with tiers and rows. At the top was Zarqawi, below him a cascade of lieutenants and foot Soldiers.

But the closer we looked, the more the model didn't hold. Al Qaeda in Iraq's lieutenants did not wait for memos from their superiors, much less orders from bin Laden. Decisions were not centralized, but were made quickly and communicated laterally across the organization. Zarqawi's fighters were adapted to the areas they haunted, like Fallujah and Qaim in Iraq's western Anbar province, and yet through modern technology were closely linked to the rest of the province and country. Money, propaganda, and information flowed at alarming rates, allowing for powerful, nimble coordination. We would watch their tactics change (from rocket attacks to suicide bombings, for example) nearly simultaneously in disparate cities. It was a deadly choreography achieved with a constantly changing, often unrecognizable structure.

Over time, it became increasingly clear -- often from intercepted communications or the accounts of insurgents we had captured -- that our enemy was a constellation of fighters organized not by rank but on the basis of relationships and acquaintances, reputation and fame. Who became radicalized in the prisons of Egypt? Who trained together in the pre-9/11 camps in Afghanistan? Who is married to whose sister? Who is making a name for himself, and in doing so burnishing the al Qaeda brand?

All this allowed for flexibility and an impressive ability to grow and to sustain losses.

The enemy does not convene promotion boards; the network is self-forming. We would watch a young Iraqi set up in a neighborhood and rise swiftly in importance: After achieving some tactical success, he would market himself, make connections, gain followers, and suddenly a new node of the network would be created and absorbed. The network's energy grew.

In warfare, you make decisions based on indicators. When facing the enemy, you estimate its tactical strength and intuit its planned strategy. This is much simpler when the enemy is a column advancing toward you in plain sight. Our problem in both the Iraq of 2003 and the Afghanistan of today is that indicators popped

"In bitter, bloody fights in both Afghanistan and Iraq, it became clear to me and to many others that to defeat a networked enemy we had to become a network ourselves."

up everywhere, unevenly and unexpectedly, and often disappeared as quickly as they emerged, flickering in view for only a moment.

We realized we had to have the rapid ability to detect nuanced changes, whether the emergence of new personalities and alliances or sudden changes in tactics. And we had to process that new information in real time -- so we could act on it. A stream of hot cinders was falling everywhere around us, and we had to see them, catch those we could, and react instantly to those we had missed that were starting to set the ground on fire.

Shortly after taking command of the JSOTF, I visited one of our teams in Mosul, the largest city in northern Iraq, which was at that time under the able command of then-MG David Petraeus and the troops of the 101st Airborne Division. Although Mosul was still less violent than some other areas of the country, it was clear that al Qaeda was organizing to aggressively contest control of the city -- and, from there, all of northern Iraq.

Our special operations force there was small: about 15 men, supported by a single intelligence analyst. They were set up in a corner of a larger base, operating quietly from a modest white trailer. Although they coordinated with the military forces and civilian (particularly intelligence) agencies on the base, operational security procedures and cultural habits limited the true synergy of their effort against AQI and the fight for the city that lay outside the base's gates.

Moreover, the few antennas that adorned the trailer's roof were unable to pump enough classified information between them and our task force headquarters (or other teams in Iraq) with any timeliness. It wasn't a marooned outpost, thanks to the remarkable team that manned the effort. But it felt like one.

That night, on the plane back to Baghdad, I drew an hourglass on a yellow legal pad. The top half of the hourglass represented the team in Mosul. The other represented our task force HQ. They met at just one nar

(Continued on page 8)

(Continued from page 7)

row point. At the top, our team in Mosul was accumulating knowledge and experience, yet lacked both the bandwidth and intelligence manpower to transmit, receive, or digest enough information either to effectively inform, or benefit from, its more robust task force headquarters. All across the country -- in Tikrit, Ramadi, Fallujah, Diyala -- we were waging similarly compartmentalized campaigns. It made our hard fight excruciatingly difficult, and potentially doomed.

The sketch from that evening -- early in a war against an enemy that would only grow more complex, capable, and vicious -- was the first step in what became one of the central missions in our effort: building the network.

What was hazy then soon became our mantra: It takes a network to defeat a network.

But fashioning ourselves to counter our enemy's network was easier said than done, especially because it took time to learn what, exactly, made a network different. As we studied, experimented, and adjusted, it became apparent that an effective network involves much more than relaying data. A true network starts with robust communications connectivity, but also leverages physical and cultural proximity, shared purpose, established decision-making processes, personal relationships, and trust. Ultimately, a network is defined by how well it allows its members to

see, decide, and effectively act. But transforming a traditional military structure into a truly flexible, empowered network is a difficult process.

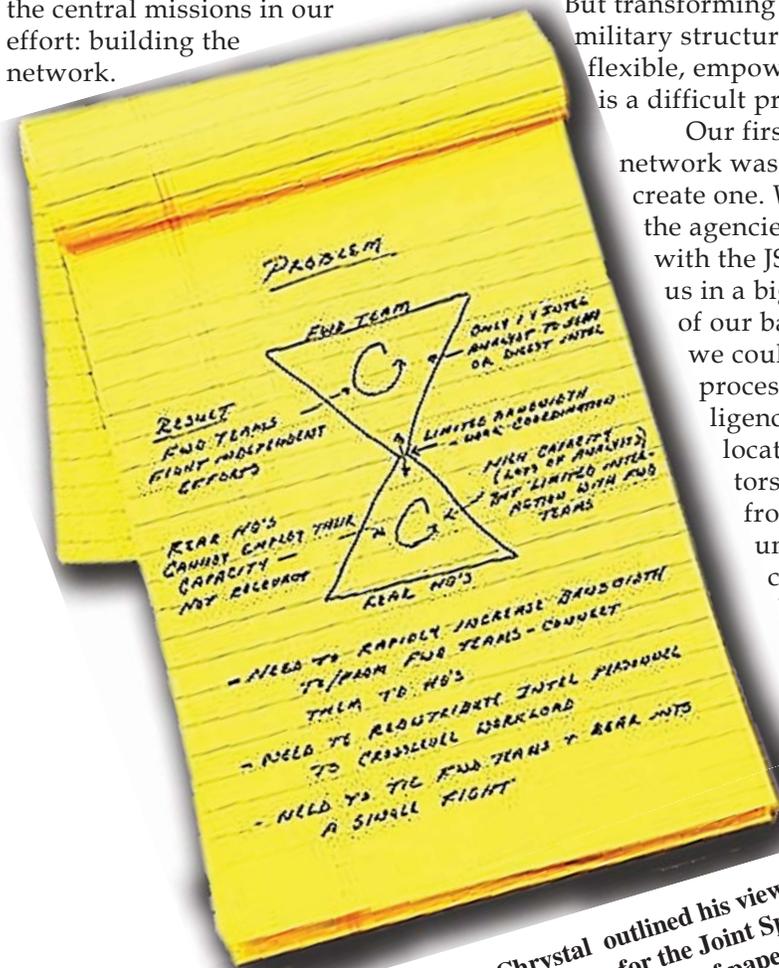
Our first attempt at a network was to physically create one. We convinced the agencies partnered with the JSOTF to join us in a big tent at one of our bases so that we could share and process the intelligence in one location. Operators and analysts from multiple units and agencies sat side by side as we sought to fuse our intelligence and opera-

tions efforts -- and our cultures -- into a unified effort. This may seem obvious, but at the time it wasn't. Too often, intelligence would travel up the chain in organizational silos -- and return too slowly for those in the fight to take critical action.

It was clear, though, that in this fusion process we had created only a partial network: Each agency or operation had a representative in the tent, but that was not enough. The network needed to expand to include everyone relevant who was operating within the battle space. Incomplete or unconnected networks can give the illusion of effectiveness, but are like finely crafted gears whose movement drives no other gears.

This insight allowed us to move closer to building a true network by connecting everyone who had a role -- no matter how small, geographically dispersed, or organizationally diverse they might have been -- in a successful counterterrorism operation. We called it, in our shorthand, F3EA: find, fix, finish, exploit, and analyze. The idea was to combine analysts who found the enemy (through intelligence, surveillance, and reconnaissance); drone operators who fixed the target; combat teams who finished the target by capturing or killing him; specialists who exploited the intelligence the raid yielded, such as cell phones, maps, and detainees; and the intelligence analysts who turned this raw information into usable knowledge. By doing this, we speeded up the cycle for a counterterrorism operation, gleaning valuable insights in hours, not days.

But it took a while to get there. The process started as a linear, relatively inefficient chain. Out of habit (and ignorance), each element gave



GEN (R) Stanley A. McChrystal outlined his view of the knowledge management situation for the Joint Special Operations Task Force on a single sheet of paper.

the next group the minimum amount of information needed for it to be able to complete its task. Lacking sufficient shared purpose or situational awareness, each component contributed far less to the outcome than it could or should have.

This made us, in retrospect, painfully slow and uninformed. The linear process created what we called “blinks” -- time delays and missed junctures where information was lost or slowed when filtered down the line. In the early days of the effort, we had multiple experiences where information we captured could not be exploited, analyzed, or reacted to quickly enough -- giving enemy targets time to flee. A blink often meant a missed opportunity in an unforgiving fight.

The key was to reduce the blinks, and we did so by attempting to create a shared consciousness between each level of the counterterrorism teams. We started by sharing information: Video streamed by the drones was sent to all the participants -- not just the reconnaissance and surveillance analysts controlling them. When an operation was set in motion, information was continuously communicated to and from the combat team, so that intelligence specialists miles away could alert the team on the ground about what they could expect to find of value at the scene and where it might be. Intelligence recovered on the spot was instantly pushed digitally from the target to analysts who could translate it into actionable data while the operators would still be clearing rooms and returning fire.

This knowledge was immediately cycled back through the loop to our intelligence and surveillance forces following the results of the raid in real time.

The intelligence recovered on one target in, say, Mosul, might allow for another target to be found, fixed upon, and finished in Baghdad, or even Afghanistan. Sometimes, finding just one initial target could lead to remarkable results: The network sometimes completed this cycle three times in a single night in locations hundreds of miles apart -- all from the results of the first operation. As our operations in Iraq and Afghanistan intensified, the number of operations conducted each day increased tenfold, and both our precision and success rate also rose dramatically.

Although we got our message out differently than did our enemies, both organizations increasingly shared basic attributes that define an effective network. Decisions were decentralized and cut laterally across the

organization. Traditional institutional boundaries fell away and diverse cultures meshed. The network expanded to include more groups, including unconventional actors. It valued competency above all else -- including rank. It sought a clear and evolving definition of the problem and constantly self-analyzed, revisiting its structure, aims, and processes, as well as those of the enemy. Most importantly, the network continually grew the capacity to inform itself.

From its birth in Iraq, both the actual network -- and the hard-earned appreciation for that organizational model -- increasingly expanded to Afghanistan, especially as our nation’s focus turned toward that theater. When I became the commander there, we set about building a robust communications architecture and worked to establish relationships with key actors, moving frequently around the country to instill the shared consciousness and purpose necessary for a networked modern army. But that was only the first part of the task. As we learned to build an effective network, we also learned that leading that network -- a diverse collection of organizations, personalities, and cultures -- is a daunting challenge in itself. That struggle remains a vital, untold chapter of the history of a global conflict that is still under way.

GEN (R) Stanley A. McChrystal is a retired U.S. Army four-star general. His last assignment was as commander, International Security Assistance Force and Commander, U.S. Forces Afghanistan. He previously served as director, Joint Staff from August 2008 to June 2009 and as commander, Joint Special Operations Command from 2003 to 2008. Since retirement, he has served on the staff of Yale University teaching a graduate seminar in modern leadership at the Jackson Institute for Global Affairs. He also serves on the boards of directors of JetBlue Airways and Navistar.

ACRONYM QuickScan

AQI - al Qaeda in Iraq

JSOTF - U.S. Joint Special Operations Task Force

Join the Discussion

<https://signallink.army.mil>

