Open-Source Warfare

by Robert N Charette via Kismo - IEEE Spectrum *Friday, Nov 23 2007, 9:45pm*
international / social/political / other press

nobody can stop the 'music'

> “What we are seeing is the empowerment of the individual to conduct war,” says John Robb, a counterterrorism expert and author of the book Brave New War (John Wiley & Sons), which came out in April. While the concept of asymmetric warfare dates back at least 2000 years, to the Chinese military strategist Sun-tzu, the conflict in Iraq has redefined the nature of such struggles. As events are making painfully clear, Robb says, warfare is being transformed from a closed, state-sponsored affair to one where the means and the know-how to do battle are readily found on the Internet and at your local RadioShack. This open global access to increasingly powerful technological tools, he says, is in effect allowing “small groups to...declare war on nations.”

On the afternoon of Thursday, 8 April 2004, U.S. troops stationed in Iraq deployed a small remote-controlled robot to search for improvised explosive devices. The robot, a PackBot unit made by iRobot Corp., of Burlington, Mass., found an IED, but the discovery proved its undoing. The IED exploded, reducing the robot to small, twisted pieces of metal, rubber, and wire.

The confrontation between robot and bomb reflects a grim paradox of the ongoing conflict in Iraq. The PackBot's destruction may have prevented the IED from claiming a soldier's life—as of 31 August, IEDs accounted for nearly half of the 3299 combat deaths reported by coalition forces. But the fact remains that a US $100 000 piece of machinery was done in by what was probably a few dollars' worth of explosives, most likely triggered using a modified cellphone, a garage-door opener, or even a toy's remote control. During the past four and a half years, the United States and its allies in Iraq have fielded the most advanced and complex weaponry ever developed. But they are still not winning the war.

Although there has been much debate and finger-pointing over the various failures and setbacks suffered during the prolonged conflict, some military analysts and counterterrorism experts say that, at its heart, this war is radically different from previous ones and must be thought of in an entirely new light.

“What we are seeing is the empowerment of the individual to conduct war,” says John Robb, a counterterrorism expert and author of the book Brave New War (John Wiley & Sons), which came out in April. While the concept of asymmetric warfare dates back at least 2000 years, to the Chinese military strategist Sun-tzu, the conflict in Iraq has redefined the nature of such struggles. As events

are making painfully clear, Robb says, warfare is being transformed from a closed, state-sponsored affair to one where the means and the know-how to do battle are readily found on the Internet and at your local RadioShack. This open global access to increasingly powerful technological tools, he says, is in effect allowing “small groups to…declare war on nations.”

Need a missile-guidance system? Buy yourself a Sony PlayStation 2. Need more capability? Just upgrade to a PS3. Need satellite photos? Download them from Google Earth or Microsoft's Virtual Earth. Need to know the current thinking on IED attacks? Watch the latest videos created by insurgents and posted on any one of hundreds of Web sites or log on to chat rooms where you can exchange technical details with like-minded folks.

Robb calls this new type of conflict “open-source warfare,” because the manner in which insurgent groups are organizing themselves, sharing information, and adapting their strategies bears a strong resemblance to the open-source movement in software development. Insurgent groups, like open-source software hackers, tend to form loose and nonhierarchical networks to pursue a common vision, Robb says. United by that vision, they exchange information and work collaboratively on tasks of mutual interest.

And just as in the software community, information technology and the Internet play a pivotal role in bringing insurgents together. The resurrection of al-Qaeda is a good example, says Brian Jackson, a terrorism expert and associate director of the Homeland Security Program at Rand Corp. “Given the structural changes that were required of al-Qaeda to adapt to its loss of Afghanistan as a safe haven,” Jackson says, “the interconnections among disparate parts of the decentralized organization that the Internet made possible have been important for its survival.”

The reliance on IT also enables open-source groups to identify and respond to problems much more rapidly than a more structured, top-down entity can—be it the Pentagon or a large software company such as Microsoft. According to some estimates, it now takes Iraqi insurgents less than a month to adapt their methods of attack, much faster than coalition troops can respond. “For every move we make, the enemy makes three,” U.S. Brigadier General Joe E. Ramirez Jr. told attendees at a May conference on IEDs. “The enemy changes techniques, tactics, and procedures every two to three weeks. Our biggest task is staying current and relevant.”

Unfortunately, the traditional weaponsacquisition process, which dictates how the United States and other Western militaries define and develop new weapons systems, is simply not designed to operate on such a fleeting timescale. It can take years and sometimes decades—not to mention many millions or billions of dollars—for a new military machine to move from concept to design to testing and out into the field. Worse, the vast majority of the battlefield technologies now wending their way through the acquisition bureaucracy were intended to fight large force-on-force battles among sovereign nations, not the guerrilla warfare that typifies the conflicts in Iraq, Afghanistan, and elsewhere.

Meanwhile, time is on the insurgents' side. Since the start of the war, the consumer-grade products on which they rely have undergone several generations of improvement. Microprocessor speeds, for instance, have leaped by a factor of at least four in that time, while the cost per MIPS—or million instructions per second, a standard benchmark for processors—has dropped by roughly 70 percent.

This past spring and summer I interviewed dozens of current and former military officers, analysts, weapons developers, and others to try to understand why the coalition forces' technological might has proved so ineffectual. Nearly everyone I spoke with agreed there is a serious mismatch between the West's industrial-age approach to warfare and the insurgents' more fluid and adaptive style. All

agreed, too, that the West will likely face more such confrontations in the years and decades ahead. The big concern, many people told me, is that once the war in Iraq has ended, the innovation that has occurred there and the lessons learned will be lost as the Pentagon returns to “business as usual”—that is, building enormously complex and costly weapons systems and training troops to fight large-scale wars.

To understand open-source warfare, it's instructive to revisit Eric S. Raymond's 1997 manifesto, The Cathedral and the Bazaar, in which he describes how a large community of open-source software hackers created the operating system Linux.

“Linux is subversive,” Raymond wrote. “Who would have thought even five years ago [1991] that a world-class operating system could coalesce as if by magic out of part-time hacking by several thousand developers scattered all over the planet, connected only by the tenuous strands of the Internet?” He likened the rise of Linux to the public marketplace of the bazaar. The programmers agreed to observe a few simple principles but were otherwise free to innovate and create. Raymond contrasted that style with the “cathedral” approach to software, in which a single organization, using highly planned, sequentially structured steps, maintained tight managerial control over every aspect of the process.

Eventually, the open-source culture would triumph over the proprietary world, Raymond argued, not because it was morally right “but simply because the closed-source world cannot win an evolutionary arms race with open-source communities that can put orders of magnitude more skilled time into a problem.”

In studying the behaviors of insurgencies in Iraq and elsewhere, as well as organized-crime syndicates and other groups, Robb noticed the many parallels to the open-source model in software. In addition to working in counterterrorism, he has also had a successful career as a software entrepreneur.

Groups like al-Qaeda resemble in some ways the classic insurgents of the past, such as the Palestine Liberation Organization, but several factors distinguish them from their predecessors, Robb says. For one, they aren't state-sponsored, which makes them harder to track down and eradicate. Being self-financed, they generate significant income from donations as well as from black-market commerce. Also, members of the group don't report to a central authority; they operate relatively autonomously, and they tend to be well educated, media-savvy, and comfortable operating in a globalized, high-tech world. And the use of information technology has given modern terrorists an operational edge their predecessors lacked.

Mimicking open-source developers, insurgent groups “hack at the source code of warfare,” Robb says. By that, he means they aren't bound by the traditional rules of military engagement; they use whatever works, with their tactics, techniques, and procedures all open to scrutiny and improvement by the community. Although such groups are weak by conventional military benchmarks—they'd clearly be outgunned and outmanned on an open battlefield—they can still threaten strong national militaries. That's because they don't aim to invade, hold, or govern territory, but rather to exert political influence by exhausting an adversary's capacity to fight back. Their preferred method of attack is to disrupt infrastructure, whether physical, financial, or political [see photos, “World at War” “System disruption is going to be the main thrust of warfare for quite a long time,” Robb predicts.

Rand CORP.'s Jackson has also studied terrorist organizations with an eye toward how they learn and share information—which he discussed in a recent report titled “Aptitude for Destruction.”

Access to the Internet, Jackson says, has given such groups “a quantum leap in capability to get their message out.”

Many of the insurgent groups in Iraq, he notes, “are very Internet-savvy in terms of using it as an information-dissemination medium.” The number of Web sites run by terrorists climbed from fewer than a dozen in 1997 to nearly 5000 in mid-2006, according to Gabriel Weimann, a professor of communications at the University of Haifa, in Israel, who has studied terrorism and the mass media. Not all of those sites pose a significant threat. Last year, a team of Pentagon analysts told Congress that of the thousands of jihadist sites they monitor, they closely watch fewer than 100—the ones they deem the most hostile.

Whereas the mass media used to control access to the public, Jackson says, insurgents now post videos and descriptions of their attacks online within hours of their occurrence, many of which are then picked up and replayed in the global media. Al-Qaeda has a media affiliate that produces slick, branded video and audio files for online distribution. The videos are often encoded in multiple formats, so you can watch them on your cellphone or play them on a big-screen television. Some insurgents are even shooting in HDTV.

Terrorist Web sites serve not only to spread propaganda but also to share knowledge among insurgent groups, Jackson says. That helps explain why the learning cycles among Iraqi insurgents are some 20 times as fast as the Irish Republican Army's were in Northern Ireland in the 1980s, according to military estimates. The SITE Institute, a group in Washington, D.C., that monitors terrorist Web activities, has documented numerous cases of technical know-how being exchanged online. These include a slide presentation posted on a password-protected Arabic-language forum purporting to teach “beginner jihad fighters” how to rig a car bomb, as well as a training manual—linked to from various jihadist forums—that claims to cover explosives, poisons, and forgery, among other topics.

To be sure, the technical information that goes up on such sites is not always to be trusted, notes Michael Kenney, an assistant professor of public policy at Pennsylvania State University in Harrisburg. “Some of the terrorist instructional manuals and online chat rooms that have received so much attention in the press are, in fact, littered with basic mistakes,” Kenney says. He had one of the world's leading explosives experts review some online training manuals. The expert found that “for every four or five recipes, one may work, [but] only a trained eye can catch” the errors, Kenney says.

Kenney also wonders how much a budding guerrilla can learn by simply reading. “Building bombs with your bare hands is still the best way to learn how to build bombs,” he says. “Shooting a firearm over and over is the best way to become a sharpshooter. These are skills that cannot really be learned from recipes that you download through the Internet.... The reason Iraq has proven to be such a rich learning environment for insurgents has more to do with practical, on-the-ground opportunities for learning that the fighting provides.”

Nevertheless, he agrees with Jackson that terrorist groups are proving to be fast learners. They're able to change their activities in response to practical experience and technical information, store this knowledge in practices and procedures, and select and retain routines that produce satisfactory results. As they gain experience, their learning cycles will only continue to shorten.

All the bomb-building advice in the world would be meaningless, of course, if the materials to build those bombs weren't also easy to come by. But they are, and terrorist groups are proving adept at using commercial, off-the-shelf technology to create effective and low-cost weapons systems.

A good example is last year's plot to smuggle common chemicals on board commercial flights using drink containers. The chemicals would then be mixed together to form explosives, which if detonated by a small charge from, say, a few modified AA batteries, could be powerful enough to bring down the aircraft.

Here again, information technology plays a crucial role. Fast and efficient worldwide distribution channels set up by the likes of Wal-Mart and Federal Express greatly simplify the acquisition of requisite components. Free from the administrative burdens of maintaining their own infrastructure, terrorist groups can spend the majority of their time on how best to achieve their collective vision.

The conflict in Iraq has become a test bed for open-source war, and the insurgents' weapon of choice is the IED. Since the beginning of the war, insurgents have rapidly improved their ability to create, deploy, and detonate IEDs. They've moved from simple makeshift explosives—old artillery shells or fertilizer—to shaped charges that can penetrate heavy armor plate and to buried explosives that can destroy a 61-metric-ton Abrams tank. In one favored mode of attack, insurgents detonate an IED beneath a military convoy vehicle, then follow up with a barrage of rocket-propelled grenades and rifle fire.

Even as coalition troops have become proficient at identifying roadside bombs, insurgents have shifted to using IEDs to booby-trap houses. “Nothing they're doing is going to win any prizes from the Department of Defense for high tech, but the stuff is deadly,” says Lawrence Husick, a senior fellow at the Foreign Policy Research Institute, in Philadelphia. “They're using a huge variety of cheaply available stuff.” One recent innovation is IED detonators made from battery-powered doorbells. The doorbells consist of crude 400-kilohertz transmitters and receivers. “They're sloppy as hell, but they are really hard to jam,” Husick says.

That unconventional style of mine warfare is something coalition forces clearly didn't anticipate, and response has been slow. Earlier this year, for instance, the Pentagon decided to spend $25 billion on mine-resistant ambush-protected (MRAP) armored vehicles, whose V-shaped hulls and raised chassis make them better than armored Humvees at fending off bomb blasts [see photo, “Help Is on the Way” The price tag includes $750 million to airlift the 12-metric-ton vehicles to Iraq, instead of sending them by ship. In August, though, the Pentagon scaled back its schedule, saying only 1500 of the planned 3900 vehicles would be delivered by year's end.

It's a race against time. As happened first to unarmored Humvees and then to armored Humvees, insurgents have made destroying MRAP vehicles a high priority—a “trophy kill,” as some observers call it. MRAP designs are already reportedly being rethought to deal with emerging insurgent tactics.

You might think that the lag time was due to bureaucratic screwups, but in fact, that's just how long the bureaucracy takes to respond. Marine commanders in Iraq first requested MRAP vehicles in May 2006. Acquisition officials reviewed the request and ultimately approved it late in the year. By April, five suppliers had demonstrated they could meet survivability requirements, production numbers, and delivery timelines, and they were then awarded contracts. But ramping up production doesn't happen overnight. Before MRAP vehicles became a high priority, the sole manufacturer, Force Protection, in Ladson, S.C., was making only about five per month.

Acquisition is even more cumbersome when the United States wants to send equipment to Iraqi security forces. Any request for equipment is first given a congressional review, which takes up to a month. Then the U.S. government has to draw up a letter of acceptance, which must be signed by the Iraqi government, after which a payment schedule is negotiated. Only then can the Defense

Department begin to procure the requested equipment—which itself takes time. Clearly, the longer it takes Iraqi security forces to get their equipment, the longer coalition forces will have to remain there.

Meanwhile, U.S. military strategy has only slowly started to move away from the objective it has had since the start of the Cold War: acquiring a technologically superior military capable of fighting (and winning) two major wars simultaneously. During the past decade, efforts have been under way to transform the military into a more agile force, one that can fight not only traditional wars but also irregular or asymmetric conflicts.

But while the overall strategy may be shifting, the dependence on high-technology weaponry has not. Creating and maintaining a high-tech force has proven both costly and time-consuming. Today, it takes 12 to 15 years to field a major weapons system, according to the U.S. Government Accountability Office (GAO). The newest U.S. Air Force jet fighter, the F-22A Raptor, was finally declared operational in December 2005—25 years after the requirement for the aircraft was approved. Although the Air Force originally planned for a force of 750 Raptors, at the current price of $138 million per plane, fewer than 200 will likely ever be built.

The weapons acquisition process is still geared toward building traditional battlefield systems like the F-22. Even after the Cold War ended—and with it, the pressure to build large numbers of complex weapon systems—decisions made decades earlier continued to prevail.

There has been no shortage of attempts to streamline weapons acquisition. Since 1975, at least 129 studies have been conducted on how to reform the process and make it more rational and responsive. Few of the recommendations have had any lasting impact, though. A March 2006 GAO report found that for the largest acquisition programs, the average estimated development time has risen from 11 years to 14 years. Even if you could design an F-22 in a single day, it would still take years to prepare the paperwork to win funding and more years of operational tests before the plane could go into full-scale production.

The financial stakes work against reform. In a report to Congress earlier this year, David Walker, comptroller general of the United States, said that annual U.S. investments in major weapons systems had doubled between 2001 and 2006, from $750 billion to more than $1.5 trillion.

Many of the defense experts I spoke with advocate a separate acquisition process to deal with the type of irregular warfare now being fought in Iraq. Robb, for one, isn't convinced that this would make much of a difference. “The big-war crowd doesn't want to understand open-source warfare,” he says.

As Upton Sinclair once said, “It is hard to get a man to understand something if his living depends on him not understanding it.”

Faced with the crisis in Iraq, the Pentagon has made a number of attempts to speed up the acquisitions process. The U.S. Army, for example, has established a Rapid Fielding Initiative to try to shorten the time it takes to get requested equipment to soldiers. That has enabled the deployment of the Advanced Combat Helmet, which offers better protection, comfort, and hearing, and an improved first-aid kit for treating bleeding and removing airway obstructions. The Army's Rapid Equipping Force identifies unconventional commercial products that may be of use on the battlefield. Industrial leaf blowers, for instance, are now being strapped on to vehicles to blow away dirt and debris from hidden bombs.

The Pentagon is also now granting certain high-priority projects “rapid-acquisition authority.” That process allowed warheads for the thermobaric Hellfire missile, used to attack caves and tunnels, to be developed in just 60 days, rather than the year it might have taken.

Then there are the robots, like the PackBot and the unmanned combat air vehicles (UCAVs), which have proved invaluable in Iraq and elsewhere. Many of these systems are not being developed as “programs of record”—although they're in wide use, they are still considered prototypes in the R&D phase. As such, they are continually being improved and refitted based on real-world experience. The companies that design the robots tend to be small, entrepreneurial enterprises, and therefore quick to respond and change. Already, some 3000 smaller ground robots have been deployed in Iraq and Afghanistan. About 1000 unmanned aerial vehicles of various stripes have also been deployed—from hand-launched, low-altitude surveillance planes to high-altitude, remotely piloted Reaper UCAVs equipped with infrared, laser, and radar targeting as well as four air-to-ground Hellfire missiles and two 500-pound bombs. These machines are probably the closest thing to an -“insurgent-resilient” weapons system that the West has.

The West's reliance on robotic war machines is certain to continue. Back in 2001, Congress mandated, as part of the National Defense Authorization Act, that “by 2010, one-third of the operating deep-strike aircraft of the Armed Forces are unmanned, and by 2015, one-third of the operational ground combat vehicles are unmanned.” The danger is that as the cost and complexity of the robots grow, they will cease to be considered “expendable” assets. Already, a four-aircraft package of Reapers carries a price tag of nearly $70 million. It's not hard to imagine the day when UCAVs will end up costing as much and taking as much time to develop as the manned systems they're intended to replace.

Growing reliance on robots also raises operational—if not ethical—questions. “What do you do when women and children come out with spray cans and hammers and start attacking your robots?” asks William Lind, a military expert with the Free Congress Foundation, a conservative think tank in Washington, D.C. “Are you going to shoot them to defend your robots?”

And so, for the most part, such shortcuts in acquisition are mere Band-Aids. The current approach effectively decouples the needs of soldiers on the ground from the process of acquiring the equipment they'll ultimately get. No sustained attempt has been made to create an insurgent-resilient model of acquisition.

What all this likely means is that when the wars in Iraq and Afghanistan finally end, the Pentagon's current “cathedral” approach will envelop robots, UCAVs, and any other interesting technology developed in the heat of battle. “As the war winds down, the forces of standardization will reassert themselves,” says Rand Corp. vice president Thomas McNaugher, an expert on defense acquisition. “That's likely to kill many of the innovations now in use on the battlefield.”

Robb says the solution is for defense acquisition to move away from what he calls “point innovations”—that is, stand-alone systems—to platform-based systems. A platform, he explains, is a collection of services and capabilities that everyone gets access to. Think of the Internet and how eBay and Google exploit it.

How would such platforms work in the military sphere? Consider a project under way at the Space Vehicle Directorate at Kirtland Air Force Base, in New Mexico. Researchers are attempting to design inexpensive “plug and play” satellites that could be fielded in six days or less. Each satellite would be built from a set of standard components that could then be quickly programmed to fit the specific mission.

To avoid getting trapped in a one-size-fits-all mentality, says Jim Lyke, technical advisor to the project and its principal electronics engineer, “We intentionally made it easy to swap out a small battery for a big battery, [an] X-band radio for a Ku-band radio, and so on.” The concept is sort of like adding components and loading software onto your PC, depending on whether you want to create spreadsheets, play games, or listen to music.

“We are waging a battle against complexity,” Lyke says. The six-day target “became a rallying theme to force us way out of our comfort zone.”

Lind of the Free Congress Foundation says it's also important to capture the innovations going on in the trenches. “There is a tremendous amount of creativity at the junior level, but there is no outlet for it. We need to richly resource sergeants and let them tinker,” he says. “The kinds of technology that are useful in these wars are what I call garage and junkyard technologies.” The original armor for Humvees, for instance, was cobbled together by soldiers in the field, who dubbed it “hillbilly armor.” Once a useful technology has been discovered, Lind adds, that information can be rapidly conveyed using the military's secure intranets. The idea is to make use of information and IT just as the insurgents do.

Meanwhile, what is happening in Iraq and Afghanistan is only a foreshadowing of the types of conflicts that Western countries will likely face in the coming decades. Insurgent learning will continue long after coalition forces have withdrawn from those countries. To face this future, it seems clear that the West urgently needs an insurgent-resilient process for developing and fielding effective military systems and tactics, along with a radical change in strategic thinking.

“We have to look outside the normal bureaucratic way of doing things,” U.S. Secretary of Defense Robert M. Gates noted at a press conference in June. “For every month we delay, scores of young Americans are going to die.” If the United States and its allies fail to embrace the need for change, they will inevitably pay the cost in both treasure and blood.

Contributing Editor Robert N. Charette is an IEEE member and risk-analysis expert in Spotsylvania, Va. His blog Risk Factor is at [http://blogs.spectrum.ieee.org/riskfactor.](http://blogs.spectrum.ieee.org/riskfactor)

Improvised Explosive Device

http://spectrum.ieee.org/nov07/5668

Cleaves Alternative News. http://cleaves.lingama.net/news/story-798.html