

# War 2.0

By Thomas Rid

Inventions can cast a seductive spell. Promising communication technologies in particular may mesmerize even serious men: "Space will be, to all practical purposes of information, completely annihilated," enthused a House Commerce Committee report published on April 6, 1838. Its authors were enthralled by Samuel Morse's recent invention, the telegraph.

One hundred and sixty years later, the internet similarly inflated expectations in politics and commerce. After the bubble burst in 2001, many disappointed entrepreneurs and investors recognized that the "new," transformed economy had been overrated and overheated. Just as the markets overestimated the World Wide Web's seemingly unlimited economic potential, the U.S. defense establishment also was lured by a techno siren song, that of network-centric operations. Widespread enthusiasm about the new, "transformed" army's seemingly unlimited military potential grew. But just as many businesses in that digitalized age could not deliver profit, the computerized force could not deliver victory. The Pentagon used its technology-driven "transformation" project in a non-social way, to link "sensors to shooters" in order to minimize reaction time. Its very ideal seemed to have been to minimize the role of fallible humans. Only now, as American soldiers are stuck in two mostly low-tech protracted guerrilla campaigns in Iraq and Afghanistan, is the military's high-tech bubble beginning to burst.

The idea of network-centric operations initially was inspired by developments in the IT-industry in the 1990s. But while today's internet industry is happily nurturing a new boom revolving around Web 2.0, the defense establishment is haplessly managing counterinsurgency and stability operations. Yet a closer look at the two seemingly separate trends brings to light striking similarities. War's

changing character is not only augmented by the emergence of the new media; the way the web and today's communication devices are used to organize lives also instructs our understanding of how killing is organized. The argument put forward here is that the web's emerging organizing principles – including a social as well as a technological dimension – increasingly govern the management of violence. The new media consequently offer both a set of new metaphors to understand the character of today's wars and a socio-technological platform that remodels the architecture of battle.

War's true transformation has a face very different from the one originally envisioned by the Pentagon's civil and military leadership, in which the force with the more expensive cutting-edge equipment would prevail. Yet let there be no misguided enthusiasm: new means of communication neither "annihilate space" nor disperse the fog of war; on the contrary, the web makes warfare even more chaotic, messy, and deadly. Just as the telegraph once did.

## Web 2.0 at war

Marked most visibly by the technologically sophisticated first war against Iraq in 1991, the U.S. Defense Department's project of military transformation was widely celebrated as a "revolution in military affairs" of historical dimensions. Never before had an army acquired such awe-inspiring technological superiority over virtually all possible adversaries. Officers all around the world adapted the basic concept of transformation, or "network-centric operations" in the military's idiom. But the movement threatened to turn into an inward-looking technology exercise, with a narrow focus on high-tech projects such as blue-force-tracker, an astronomically expensive system to monitor the actual position of all American forces in real-time, or high-resolution overhead imagery and even live video-feeds, beamed into command headquarters by satellites and drones. Real-time signal intelligence from the sky was to be instantly connected with massive firepower on the ground to enhance the 21st-century warfighting machine's efficiency and lethality.

This may be important, but it rather misses the

point in modern war: the enemy's resort to asymmetric means of struggle, the significance of human interaction and social contacts, of improvisation, endurance, commitment, and trust. This is a lesson soldiers on the ground are painfully learning in Iraq: "I would trade every satellite in the sky for one reliable informant," said Army Lieutenant Colonel Ross Brown, who commanded a cavalry squadron in the 3rd Armored Cavalry Regiment south of Baghdad.

<sup>1</sup> The local insurgencies in Iraq, Afghanistan, and Lebanon, as well as global militant jihadis, rely on tacit and trusted social networks, not on attackable fiber-optic networks. As a consequence, the burgeoning but introspective debate about transformation in today's most advanced armies has largely been replaced by a more down-to-earth debate about counterinsurgency warfare. In December 2006, the Army announced plans to cut its Future Combat System by \$3.3 billion and to scrap the transformational Land Warrior program. In the same month, for the first time in more than two decades, a joint Army-Marine Corps publication on counterinsurgency was issued; its lead author now commands America's troops in Iraq.

Yet the web is back. And once more the private sector is setting the trend. Today some of the largest IPOs again pour money into web-based companies' pockets. Google epitomizes the web's new bloom. In early 2007, the firm's market capitalization surpassed \$150 billion, nearly four times that of Lockheed Martin, the world's largest defense contractor. This time business models appear more solid, and profit is delivered. But there is one persistent change: Individuals have moved to the center of attention. Not only as buyers, but as vendors, advertisers, developers, designers, and producers. Media professionals coined the phrase "Web 2.0" to describe this new trend. Its effects have changed our lives: maps, diaries, contacts, telephone calls, private financial transactions, photo collections, videos, music, shopping, flea markets, dating, and even mourning are today done electronically as much as manually.<sup>2</sup> An increasing share of interactions both noncommercial and commercial are *between* individuals, not between consumers and collective entities, like companies or states. A historical precedent does not exist. Just like in the

peaceful metropolis with its wireless-capable cafés and parks, informal social networks determine success on remote battlefields, sometimes interacting through computers and cell phones, sometimes on local houses' front porches. That applies to the counterinsurgent, and even more so to the insurgent.

Insurgencies, terrorist attacks, and urban operations, to be sure, are not a video game fought virtually on screens. Suicide bombers are creating real carnage, roadside bombs are ripping apart real human beings, and nightly cordon-and-search operations are humiliating real families – whether or not there is a nearby cell phone or internet access. Acts of violence may or may not rely on fiber-optic networks. But whether in a hierarchical army or in a decentralized insurgency with a scattered, blind-cell setup, acts of violence are always organized by social networks – and they target the adversary's social coherence, his ability to develop, execute, and maintain a political will. The web, ever more focused on social networking, changes the equation on both sides.

Drawing analogies between two vastly different spheres is risky. But to come to grips with a new or significantly altered phenomenon, we rely on metaphors. To see the ways in which irregular warriors and traditional officers use the web to their advantage, the internet industry itself offers the richest and most useful set of analogies. The following principles apply, to a varying degree, to both the insurgent and the counterinsurgent. The descriptions are intended to be thought-provoking, not as exhaustive and definite.

(1) In the media industry and in warfare, the initiative and innovations increasingly come from small start-ups on the *lower and middle-management level*, a norm that applies to Google, al-Qaeda, and the U.S. Army.

(2) Consequently, ordinary users must be treated as co-developers who can come up with a new product or add a competitive edge to it, not merely as consumers. Tactical battle guidelines and lessons-learned essays benefit from user-developed suggestions and improvements in a way that is analogous to the "patches" of open-source applications or Wikipedia's articles, called *peer-production* in the industry's jargon.<sup>3</sup>

(3) User contributions based on *open standards*

become decisive for dominance on the marketplace as well as in the battlespace. Linux is the media equivalent of the IED: successful beyond expectations, as "scripts" or explosive designs can easily be accessed and adapted to each application's specific needs; successful tactics become commoditized.

(4) As a result, the distinction between the final product and its development phase becomes obsolete, an effect that is known in industry as the "*permanent beta-version*": both counter-ambush tactics as well as browser-based email platforms, to pick two examples, are permanently updated and never graduate to a finalized version.

(5) It follows that the *acceleration of development cycles* becomes a way to out-manuever the competition, and to gain and maintain the initiative over the adversary's actions; software developers correspondingly adapted their build-and-release management to embrace a more efficient "release early, release often" philosophy.

(6) Simple technologies and systems with low adaptation costs have a competitive advantage, called "*loose coupling*," a term widely used by programmers for friction-free linking of formerly incompatible IT-systems through a common semantic framework. Such systems are more "adaptable to the unexpected."<sup>4</sup> This equally applies to insurgents and militant networks that easily transfer their successful tactics and innovations to other groups, a trend that sharply distinguishes them from technologically sophisticated armies whose "interoperability" diminishes as their systems grow more complex.

(7) Whether triggered by advertisements on obscure pages or by ambushes on obscure highways, many small but numerous hits add up to significant volumes that can have decisive consequences, an effect referred to in the industry as "*The Long Tail*."<sup>5</sup>

(8) As a result of the large numbers of contributors taking the initiative on their own, in the business of software and warfare, finally, command and control takes the form of *syndication* rather than coordination.

The transfer of these principles from software to warfare requires abstraction – and possibly goodwill. Several of the analogous dynamics have long dominated guerrilla movements and predate the internet by centuries, which at first glance

merely seems to offer new comparisons for old phenomena. Popular uprisings, low-tech improvisation, and the steady infliction of costs, after all, characterized most rebellions in history. Yet even these perennial principles of war did not remain unaffected by the arrival of the internet in theater.

## Insurgency and counterinsurgency

To appreciate the relevance of social networks, and consequently the web's impact, some background in counterinsurgency theory is necessary. An insurgency is a struggle for control of a political or economic space. A government or a coalition of states tries to maintain the status quo, and a sub-state actor or a group of nongovernmental challengers fight to change the status quo. "Small wars," "low-intensity operations," "asymmetric wars," and "guerrilla wars" are interchangeable terms. Insurgent groups can also have an interest – political, religious, or economic – in a perpetuated state of ungoverned spaces, such as some poppy-growing warlords in Afghanistan or martyrdom-seeking mujahids in Waziristan. Then the counterinsurgent is contesting the status quo, and the resistance may bitterly defend it. In any case, the counterinsurgent's political objective is to create a stable government system and the rule of law. The insurgent, by contrast, may or may not have a clear political war aim.

The classical theory of counterinsurgency, in a nutshell, is simple: the counterinsurgent competes with the insurgent for the ability to win the hearts, minds and acquiescence of the local civilian population. David Kilcullen, an Australian counterinsurgency practitioner, wrote an outstanding paper on the subject, "Twenty-Eight Articles." Shortly after its publication in 2006, it made the round in U.S. Marine leadership circles, and got the author a job as consultant for the top U.S. commander in Iraq. "In this battlefield popular perceptions and rumor," Kilcullen observes, "are more important than a hundred tanks."<sup>6</sup> He is able to hark back to decades of battlefield-hardened ideas and insights. The communication revolution, however,

adds a new quality to this classic tenet.

Centuries of colonialism were characterized by countless counterinsurgency campaigns in alien lands around the globe, and many colonies' struggles for independence were long and bloody. So it comes as no surprise that the classic works on guerrilla war were either penned by Europeans or their former adversaries. The British had Charles Caldwell, a royal major general, who took part in the Afghanistan Wars as well as the Boer Wars and captured his insights in *Small Wars*<sup>7</sup>; T.E. Lawrence, an advisor to insurgents against the Ottoman occupier in Arabia, published the legendary book *Seven Pillars of Wisdom*, condensed "as stalking horses for beginners" in 27 *Articles*<sup>8</sup>; Major General Frank Kitson, one of the crown's best practitioners of small wars, wrote *Low-Intensity Operations*.<sup>9</sup> Several French officers published books on their experiences after the fourth republic's tough campaigns in Indochina and Algeria. The two best known are Roger Trinquier's tough *Modern War* and David Galula's *Counterinsurgency Warfare*.<sup>10</sup> Both were republished in 2006, one with a foreword by Eliot Cohen, the other by Bruce Hoffman, two of America's most respected voices on war and terrorism. And then there are those from the other side, the insurgency's side. Their names bear the weight of history: Mao Zedong's innovative ideas on the role of the peasantry in guerrilla warfare, Che Guevara's notion of the *foco*, Vo Nguyen Giap's writings on the various stages of an insurrection.

Some of the classics' tenets are applicable today, some are not. Insurgencies remain protracted struggles. They are still characterized by an asymmetric resource distribution and a specific set of tactics employed by the weak against the strong. Guerrilla forces old and new are highly mobile, mostly shun open confrontation, and prefer hit-and-run operations. The insurgents usually are motivated by a superior cause, be it political or religious, and they rely on the financial, logistic, and ideological support of third groups. But here the differences already begin. Colonialism's wars of independence were focused on one country or a limited region, and the local population was their most important base of support. Today's insurgencies may still target civilian populations, but their support base is

likely to be global; they operate in cities rather than in deserts and forests; they may not have a strategy or a political objective at all; and, once the larger movement is weakened, its remnants may still have access to sufficient support, resources and weapons to remain dangerous and transform into a terrorist organization. Al Qaeda itself was born when two insurgencies joined forces: bin Laden's Arab radicals, who supported the Afghan mujahideen's successful war against the Soviet occupiers, and the Muslim Brotherhood's and Ayman al-Zawahiri's unsuccessful uprising against the Egyptian government under Nasser, Sadat, and Mubarak.<sup>11</sup>

In both classical and modern insurgencies the interplay between military and civilian spheres is very complex. Mao wrote about the "relationship that should exist between the people and the troops" and introduced his famous analogy: "The former may be likened to water and the latter to the fish who inhabit it."<sup>12</sup> Consequently, as guerrilla fighters are hiding within the population, it becomes very difficult to distinguish between combatants and non-combatants. "No physical frontier separates the two camps," noted Trinquier. The line of demarcation between friend and foe passes through "the very heart" of the nation, it separates villages, and even divides families, he wrote. Intelligence about the insurgency is notoriously hard to gather. It may not be classified secret but kept in denied areas, physically or electronically. The closer the informal ties between the insurgent and host society, the harder the insurgency is to penetrate and the easier it becomes for the insurgent to "control the masses." Consequently, it is the aim of the counterinsurgent to isolate the insurgency and undermine its standing in the population. The counterinsurgent shares with the population an interest in stability, security, and the rule of law. The rebels, therefore, can have an interest in the opposite - terror, violence, and anarchy. The reign of chaos demonstrates to civilians that the occupier, or the government, cannot protect them. This lends credibility to the insurgent's cause. In such a situation, civilian tasks will have to be performed by officers to prevent or break a vicious circle. Galula spells this out best:

To confine soldiers to purely military

functions while urgent and vital tasks have to be done, and nobody else is available to undertake them, would be senseless. The soldier must then be prepared to become . . . a social worker, a civil engineer, a schoolteacher, a nurse, a boy scout. But only for as long as he cannot be replaced, for it is better to entrust civilian tasks to civilians.

As Trinquier notes, only the "combination of political, economic, psychological and military measures" will be effective in a stabilization operation. This requires a unified command, or at least a unity of effort; "directing the operation from beginning to the end," in Kitson's words, is essential.

In modern counterinsurgencies the problem of unity of command is confounded drastically. Actors with a critical role for an operation's success abound: multinational components of a military coalition, governmental and non-governmental development agencies, international organizations, local actors, the regional and international media. With this plethora of actors, a unity of command is not workable any more, and should be replaced by a "unity of purpose."<sup>13</sup>

This has conceptual consequences. Today army doctrine in the largest NATO countries elevates "support" to the same level as "offense" and "defense." Adding a third leg to this classical dichotomy is a radical move, particularly if viewed against traditional strategic thinkers like Carl von Clausewitz. Not to compel the insurgent to do our will, to paraphrase the Prussian, but to get the political support of the population is the primary aim in counterinsurgency; war, then, is not the continuation of politics by other means, but by the same means. The two sides politically compete for social networks with the population. French theorists beyond the commissioned officer ranks score higher in contemporary military thinking than many would expect. The U.S. Army's and the Marine Corps' 2006 Field Manual on Counterinsurgency - COIN, for professionals - introduces left-leaning sociologist Pierre Bourdieu's concept of "social capital" as one of four major forms of power in a society (the others being coercive force, economic resources,

and authority). An individual or a group owns social capital if it has the power to utilize social networks to advance his or its interests and goals. The counterinsurgent must identify the individuals who have social capital and study how they attract and maintain followers, according to the manual. Counterinsurgency is a competition for trust, for informal networks, for "social capital." The web and mobile phones increase the return on social capital. As a result, the counterinsurgent must "possess the training, capability and will to fight on *cognitive terrain*," as a U.S. Army journal put it.<sup>14</sup> This cognitive terrain is landscaped and sometimes eroded by a corrosive information environment.

The main texts on small wars and guerrilla campaigns may recognize the effects of propaganda, mobilization, and political loyalties. But Mao, Galula, and Kitson all fought and wrote before the arrival of the internet. Even David Petraeus's famed and much reviewed new American COIN doctrine is largely silent on the internet's role in the "long war." The insurgents, by contrast, are not. And neither are the mid-level U.S. commanders who have to deal with the consequences. Today's insurgencies have moved financial transactions, recruitment, training, clandestine communication, and even operational planning into a virtual hinterland — beyond the control of counterinsurgents or other governments.<sup>15</sup> "Classical counterinsurgency theory," Kilcullen pointed out in *Survival*, "has little to say about such electronic sanctuary." It even has little to say about the role of television in guerrilla war.

## A wet environment

**T**he first American experience with a new brand of counterinsurgency warfare was Somalia. On December 9, 1992, an amphibious landing of U.S. troops at an African beach near Mogadishu marked the launch of operation Restore Hope. As the soldiers went into the hostile environment, they expected, if anything, to meet enemy resistance. The Marines did not find what they expected. "Get the f--- down, you wanna f--- me to blow your f---ing head off," one of the servicemen recommended to a young American woman. She had her face in the

dirt and a gun at her head in split seconds. Donatella Lorch, a war correspondent, was awaiting the amphibious landing along with a battalion-sized force of reporters.<sup>16</sup> In retrospect Lorch defended the soldiers, saying that it was not the Marines' fault, but blamed it on "a bit of a lapse in communication." Robert Oakley, the U.S. ambassador with an important role in the entire UN operation, had briefed a group of reporters at the U.S. military base in Somalia announcing that an amphibious landing was scheduled for about midnight. If the reporters would like to be present and cover the event, they should cross the security gates without their Somali translators, he advised. Nobody, though, had warned the approaching Marines. When they came ashore, the beach resembled a movie set rather than a real strip of African beach: Cameras, bright television lights, and journalists trying to bring the clandestine landing to world attention.

The lesson was clear. The old media had become a permanent feature of the battlefield. "There is no longer a question of whether the news media will cover military operations," an officer graduating from the Army War College argued in his thesis. "As in Somalia, journalists will likely precede the force into the area of operation; and they will transmit images of events as they happen, perhaps from both sides of any conflict." Attempts to leash the media would not be feasible anymore; "efforts at control are meaningless."<sup>17</sup> Soon, joint and service doctrine would acknowledge the new realities. By the mid-1990s the Pentagon began to probe the embedding of reporters with military units in Bosnia. The *Wall Street Journal's* Thomas Ricks, for instance, traveled with the 1st Armored Division into hostile territory. Because control of the media was not an option any more, the Army reluctantly opted for cooperation.

Culturally and historically, the Marine Corps had a more relaxed attitude toward reporters on the battlefield. As a light expeditionary force composed of air, naval, and land components, the Marines have felt themselves to be under constant pressure to legitimize their existence as a separate service; they were culturally "paranoid," in the words of one of their generals, that they might one day be dissolved. As a result, the Marines regarded their excellent

reputation with the American people as existential. The Corps, its officers are taught, exists not because America truly needs it, but because the American people want it.

As a result, the Marine Expeditionary Force under General Walt Boomer, a one-time public affairs officer, managed to get excellent coverage during the 1991 Gulf War. The Army, by contrast, stonewalled. Chief warrant officer Eric Carlson had devised a way of getting the news from the 1st Marine Division to the rear in minutes. "We regarded [the media] as an environmental feature of the battlefield, kind of like the rain. If it rains you operate wet." The smallest of the U.S. military services with its specialization in amphibious operations excelled in this kind of "wet" environment, and the Marines got a disproportionate share of the coverage, notwithstanding that the Army in the northwest was doing the harder job executing the famous "left hook," one of the largest tank battles in the history of warfare. Jamie McIntyre, the Pentagon correspondent of the network that rose to global fame in the Gulf War, later used the same comparison: "Wherever commanders go, they should plan for CNN. Like the weather, we'll always be there - just another feature on the battlefield terrain." What is most remarkable about McIntyre's and Carlson's statements is that they were made in the early 1990s.

Communication between the soldiers at the front and their families at home still had its classical features in 1991. It was time delayed, narrated (not illustrated), and largely reliant on logistics provided by the military. Soldiers received field mail, and they stood in long lines at rear bases to call home. Neither the internet, nor its more sophisticated second incarnation, had yet arrived on the scene. Mobile phones were still the exception among the press corps, not to mention local civilians in the area of operation. Videophones did not exist. Blogs were unheard of. Chat rooms still evoked images of elderly ladies clustered around coffee tables. When America went to war with Saddam Hussein the second time, the information environment had undergone a drastic revolution of historic magnitude. Two trends demonstrate the sea change.

First, soldiers became journalists. Abu Ghraib was only the peak event that brought a general trend to popular attention. Enlisted soldiers

carry mobile phones, digital cameras, and they have access to the internet at their bases. Most of them write emails to their friends and family back home, occasionally attach a picture. Some publish their thoughts on blogs to anybody who is interested and upload their images and videos. Chris Missick, 24 years old and with the Army's 319th Signal Battalion, was one of those online chroniclers. He wrote the blog *A Line in the Sand*. Missick candidly describes and questions the effects of his leisure activity:

Never before has a war been so immediately documented, never before have sentiments from the front scurried their way to the home front with such ease and precision. Here I sit, in the desert, staring daily at the electric fence, the deep trenches and the concertina wire that separates the border of Iraq and Kuwait, and write home and upload my daily reflections and opinions on the war and my circumstances here, as well as some pictures I have taken along the way. It is amazing, and empowering, and yet the questions remains, should I as a lower enlisted soldier have such power to express my opinion and broadcast to the world a singular soldier's point of view?<sup>18</sup>

The spectrum of military weblogs, or milblogs as they are called in the community, is as broad as American society and the soldiers and officers that are recruited from it. Grey Eagle is the name the writer of "afemalesoldier.com" has given herself. She describes herself as a mother of two sons, serving in the 101st Airborne Division as a medic. Major Michael Cohen, a doctor in a combat support hospital near Mosul, had his blog shut down after he gave too many details of a suicide bomb attack just before Christmas 2004. "Levels above me have ordered, yes ORDERED, to shut down this website," the doctor complained in his last posting.

The online diaries are only part of the larger picture. "Today, every soldier has a cell phone, beeper, game device, or laptop, any one of which could pop off without warning. Blogging is just one piece of the puzzle," said Lieutenant Colonel Christopher Conway, a DoD public affairs officer. Indeed digital cameras and mobile phones have had

a politically more significant effect so far. On October 25, 2006 *Bild*, Germany's most popular daily tabloid, published five pictures that shocked the country. They showed German soldiers posing with body parts in Afghanistan, with a skull as a souvenir or a hood ornament. One soldier, his pants down, had himself photographed with a cranium in a sexually explicit position. As in the case of Abu Ghraib, the Bundeswehr's scandal images were dated, digitally photographed by low-ranking soldiers, and only unfolded their devastating political impact after they spilled over into the mainstream media.

Second, not only soldiers are reporting from today's war zones; civilians do as well. In Iraq, rising levels of violence force families to stay indoors and deal psychologically with the death, robberies, kidnappings, and explosions on their own. Writing, for many, becomes a way to deal with the stress. "You have two choices—take a valium, or start a blog," wrote a 24-year-old Iraqi woman who opted for the latter. The former computer programmer chose the nom de plume "Riverbend," and started the diary *Baghdad Burning*. "That's the beginning for me, I guess," she commenced on August 17, 2003, anonymously. Today she is one of the most prominent Iraqi bloggers; her gripping first person accounts have made it into two books and into the *New York Review of Books*. She covers many aspects and details of civilian and political life in Iraq. Islamist militias sending Kalashnikov bullets by mail to force some of Baghdad's residents out of their homes; women, even female Christians, increasingly wearing the all-black hijab as a protective device; the popular reaction to Saddam Hussein's death sentence; and everyday issues like electricity supply. On August 19, 2003, just hours before a large bomb destroyed the UN compound in Baghdad and prompted the world body's pullout, the young author published a more representative account of her daily frustration:

Today a child was killed in Anbar, a governorate north-west of Baghdad. His name was Omar Jassim and he was no more than 10 years old, maybe 11. Does anyone hear of that? Does it matter anymore? Do they show that on Fox News or CNN? He was killed during an American raid—no one knows why. His family are devastated — nothing was taken from the house because nothing

was found in the house. It was just one of those raids. People are terrified of the raids. You never know what will happen – who might be shot, who might react wrong – what exactly the wrong reaction might be . . .

The weblogs' lifespan and the frequency of contributions vary, as do their political positions. In that respect they mirror the military's blogs. Some, like *Iraq the Model*, are pro-American. Two of the three Fadhil brothers posting on that blog even met President Bush in the White House during a sponsored tour of the United States. Others, such as the author of *A Star From Mosul* or *Sooni* and dozens more hide their real names for security reasons. Salam Pax, an architect and translator who started publishing his diary online under Saddam, revealed his identity to a small number of journalists; he got very high visibility in the American media. Some reviewers in the mainstream media even called him the "Anne Frank of the war in Iraq."<sup>19</sup> In the insecure and terrorized environment of wartime Iraq, it becomes increasingly difficult to work for professional reporters. That resulting narrative void is increasingly filled by detailed first-person accounts published online. Freely available blogging software is currently being improved to allow publication in Arabic. As the internet penetration in the Middle East increases, and news consumption patterns change, the current dynamic will doubtlessly gain momentum.

*A Line in the Sand*, the German skull affair, and *Riverbend* exemplify a larger shift. Investigative journalists do not have to be present to have an impact. The *Columbia Journalism Review*, the profession's leading periodical in America, jokingly but tellingly quoted Thomas Dworzak of Magnum suggesting that Lynndie England, the female soldier in some of Abu Ghraib's scandal pictures, should have won a Pulitzer Prize. Indeed the journal has a point. The new media, to paraphrase CNN's McIntyre, will even more, like the weather, always be there – just another feature on the battlefield terrain.

But this insight still falls short of appreciating the real and strategically more significant change. Understanding the media and the internet as a permanent feature of the battlespace is progress, certainly. It took

decades for the U.S. defense establishment to fully realize the implications. But this metaphor's mindset is stuck in the first digital age, in the old paradigm. In the first digital age the breakthrough was an accelerated, instantaneous information flow: CNN's Peter Arnett on the Al Rashid Hotel's roof in 1991, or his colleague Walter Rodgers in an Abrams tank in 2003, broadcasting live. But their coverage was still traditional broadcasting, a one-way street, delivered by a large company. The second digital age, by contrast, is marked by interactive communication, a two-way street, frequented by individuals. The consequences are profound. In guerrilla warfare, the fish is not swimming in the ocean any more. It is, if one likes to stick to the metaphor, rather using the water as part of its fabric, more like a jellyfish. The information environment does not stay external to the organization any longer, neither for the U.S. Army nor for its enemies. It is flooding the hierarchy from the bottom up, and enabling new forms of networked organizations. Consequently it is, in the army's case, more appropriate to look at the wet environment as an innovative mode of internal communication, or, in the case of a militant networked organization, as its lifeblood, or operating system.

## The U.S. military connects

**T**he American armed forces are the most modern and best-equipped military organization on the planet. They are also the world's most intellectual and prolific army; its officers fight and write. Each service has several professional periodicals; the best ones are the Navy's *Naval War College Review*, the Marine's *Marine Corps Gazette*, the Air Force's *Airpower Journal*, and the Army's *Parameters*. In the 1950s, one such publication, *Military Review*, explicitly mentioned the journal's mission on each edition's first page. "The *Military Review* has the mission of disseminating modern military thought and current Army doctrine concerning command and staff procedures of the division and higher echelons and to provide a forum for articles which stimulate military thinking." The quality of the articles in those journals varies, but often it is stunningly high. Analytical, critical, constructive, they foster a culture of

open dialogue on issues of relevance to commanders.

So it comes as no surprise that some officers quickly saw Web 2.0's value as a publication platform. While the Marine Corps was traditionally better at external public affairs, the Army took the lead in harnessing the second digital age's new gadgets for its internal purposes. The two prime examples are CompanyCommand.com, which caters to the Army's approximately 3,300 current company commanders, and PlatoonLeader.org, a highly successful learning platform for the land force's circa 12,000 platoon leaders.

The websites' purpose is to facilitate dialogue among junior leaders and optimize the organization's ability to adapt to an ephemeral operational environment. The conversation takes place on "on front porches, around HMMWV hoods, in CPs [Command Posts], mess halls, and FOBs [Forward Operating Bases] around the world," the welcome statement says. The front porch is a hint at the website's founding history. At the end of the 1990s, the two captains Nate Allen and Tony Burgess both commanded companies in separate battalions of the same brigade, based in Hawaii. They happened to be next-door neighbors and spent many evenings on their Hawaiian front porches comparing notes. "How are things going with your first sergeant?" they would ask, or: "How did your company live-fire work out?" Realizing the positive impact of their peer conversations, the two majors wrote a book and posted it on a website. Through this initial publication they got in contact with another captain who proposed to model a website on alloutdoors.com, an online switchboard for hiking and survival advice, such as how to skin a squirrel. Allen and Burgess, together with a dozen more captains, among them Pete Kilner and Steve Schweitzer, decided to adapt the outdoor model and go ahead. "Such a site for company commanders would replicate, in cyberspace, their front porch," as Dan Baum observed in *The New Yorker*.<sup>20</sup> The active-duty entrepreneurs did not ask the Army for permission, nor for financial support, and they registered their project with a .com address, not on the U.S. military's .mil internet domain.

Soon the Army discovered the value of the sites, and included them in its official information network. Army Major General Peter

Chiarelli, then commander of the 1st Cavalry Division, started another site, CavNet initially, that ran on the U.S. military's "Secret Internet Protocol Router Network," or SIPRNET. The secure system is built on hardware that is separate from the civilian internet, and only accessible from special computers. SIPR's downside is that it is not as widely accessible as the internet. In Iraq it is available at the battalion level, but not at the company or even platoon level.

CompanyCommand.com grew to 6,200 members in 2006, when the site was viewed about a million times. "Today's army is changing so fast, that people at the high end don't always know because they haven't lived it," said Schweitzer, one of the site's administrators. For the first four years the internet site was entirely open to the public, and to the enemy. On February 8, 2004, Pentagon correspondent Thomas Ricks published an article in the *Washington Post* that prominently features the site. Overnight, the traffic skyrocketed. Its founders - not the Army - then decided to limit access to the site to professional U.S. soldiers, mostly captains.<sup>21</sup> The closure, Kilner points out, made the online community much more powerful and much more successful. "It's not just information; it's a personal story, and commanders are able to connect with their peers who share their knowledge. The forum fosters a powerful sense of shared purpose among members." It works not unlike MySpace: There are profiles with photos, bios, and mostly information on a soldier's professional background, all focused solely on being a more effective company commander. "The commanders see that the forum really is by and for them. They see others who share their challenges and experiences; they see their own face and those of their comrades, and that deepens their sense of professional identity. The learning that occurs in and through the online connections," Kilner said, "has a real impact on the war."<sup>22</sup>

The private initiative is today partnered with in the official Battle Command Knowledge System, the Army's institutionalized system of chat-rooms and internet blackboards, and is supported by the United States Military Academy and government grants. Yet the establishment understood the site's logic of a peer-to-peer culture that generates commitment. "We don't want to over-

control," said William Wallace, V Corps commander during the invasion of Iraq and now head of the Training and Doctrine Command, TRADOC. "There's a certain amount of pride in these communities in thinking that they operate outside the institution."<sup>23</sup> The institutional Army does not interfere with the operations of the CompanyCommand and PlatoonLeader sites.

The Marines prove the Army right. In May 2006, 2nd Lieutenant Andrew Schilling published an article in the *Marine Corps Gazette* which scored in one of the magazine's essay contests. "It is hard for a Marine to admit when the Army does something better," he writes, and goes on chastising the Corps for not making better use of peer technology, such as CompanyCommand and PlatoonLeader. The sites, the junior officer argues, are "superior to anything the Marines have because they treat their users as peers."<sup>24</sup> This is not to say that the Marines do not use the internet at all, but they do so outside the service's control and awareness. Schilling goes on describing how his platoon, just as many others in The Basic School (TBS), used an internet site on a private server to keep track of each other, provide study assistance, post photos, and to organize the platoon's activities. The young officers share their gouge online – jargon for tips, templates, study guides and the like. Navygouge.com is one of those sites.

The new media's use on the battlefield is not limited to the internet. "Most value is not created online," said Kilner. "It's in the chow hall, it's on the Humvee." The online part merely amplifies the face-to-face interaction. The CompanyCommand team, for instance, just installed a podcasting capability and plans to equip commanders on their way to Afghanistan with new iPods, fully loaded with video-podcasts interviews with fellow commanders on their way out. Cell phones and private digital cameras are used both for documentation and calling home. Commercial gadgets, sometimes superior to the Army's own equipment, are increasingly used to gather and document intelligence. "Take pictures of everything and even, more importantly, everyone. The right photo in the right hands can absolutely make the difference," one captain recommended online. One particularly impressive example is the use of Google Earth by some U.S. officers: The mapping tool is used in Iraq to

document the personal conversations between locals and soldiers. After a patrol returns back to base, it becomes possible to add content to the map and document relevant details of conversations with civilians and local leaders, and so create a spatially and temporally mapped track-record of trusted or problematic relationships that can be shared with other soldiers.

One effect is that today's wars are the best documented operations in history, in all their facets, including the ugly ones. And these may even be documented by the troops themselves: by the Bundeswehr soldiers in Kabul, by U.S. Army reserves in Abu Ghraib, and by British combatants in Camp Breadbasket. And here again, the boundaries between the technology's external and internal use are blurring. War leaves a heavy psychological footprint on its participants, on raided families or ambushed convoys. The personal strategies to deal with this luggage are very different. Some retreat and do not talk about what they saw and did their entire lives; some do the opposite and publish blogs or leak images they find morally repugnant to the press, even if they were made for internal consumption only. Just enter "Iraq" and "IED" as a search term on Flickr, a public photo album, on YouTube, a public amateur video collection, or on MySpace.

But the positive effects of this development should not be overlooked; in fact, they outweigh the negative ones. Junior military leaders recognize this. "Our enemy is already using IT to his advantage. Information about terrorist targets, schematics, tools and even how-to manuals are readily available on the web," Schilling wrote. "It is time for us to do the same." Others mirror this demand. "If we don't mirror the insurgency with our social networking and rapid transfer of knowledge, then soldiers' lives are put at even greater risk. Insurgents watch our forces closely, and learn what tactics are effective. We must do the same," said Ron Dysvick, who oversaw the design and implementation of the Army's Battle Command Knowledge System.<sup>25</sup> Arguably the American military – and some of its NATO partners – have already begun to go down this road. Often, though, without the explicit consent or control of its senior general officers. The new counterinsurgency doctrine has recognized this

trend:

Even the U.S. military is sliding towards a network organization as junior leaders use cell phones and internet connections to solve problems and resolve conflicts without going up the chain of command.<sup>26</sup>

The trend is best illustrated by the Army's response to the remarkable history of one the Iraq War's most deadly weapons, the IED.

## Sophisticated low-tech: IEDs

**I**n Iraq, the American Army was forced to innovate tactically against its will by a remarkably adaptive enemy. The insurgency's most effective weapon is the roadside bomb. Its fast rhythm of the changing tactics and counter-tactics illustrates the altered organizing patterns of war in the second digital age.

The political context matters here. The administration's stunning lack of planning and its dismal management of what initially had been called the "post-combat phase" is now well documented.<sup>27</sup> After the regime fell in April 2003 and the "mission" was prematurely declared accomplished, an absence of strategic guidance characterized the following months: a vacuum for Iraqis to seize the initiative. Public buildings were looted, weapons caches emptied, law and order, however repressive it was under Saddam, broke down. When action was taken, the Iraqi Army dismantled and de-Baathification enacted, it sent large numbers of trained and humiliated fighters into unemployment. Humiliating entire families in nightly "cordon-and-search" operations and, in some areas, interrogating nearly all fighting-aged male Iraqis did not help to win the civilian population's hearts and minds either. A dangerous mixture of disappointment with the new occupier, spreading anarchy and crime in a society divided along sectarian lines, ready availability of huge stockpiles of weapons, and a constant trickle of radical foreign fighters entering the country through its unprotected borders, began to energize the insurgency. The coalition's lack of leadership and strategic vision trickled down the military's hierarchy. Clear orders were absent.

Even the commander's intent, a senior leader's concise statement about the purpose of an operation and basis of any "mission command," remained utterly unclear. Yet the situation on the ground required tactical action. The occupiers had to react; it was *Auftragstaktik* without the *Auftrag*, or mission.

Still, despite the confusion, the nascent insurgency faced the most technologically sophisticated army in the history of warfare. The fighters had to match technology with cunning. Two months into the occupation, one of the classic weapons of an insurrection entered the stage: the Improvised Explosive Device, or IED. The term was new, but the idea was not. In Vietnam, booby-traps caused many casualties; the mujahideen in Afghanistan even used bicycles filled with explosives against their Soviet occupiers. Concealed bombs are the weak's weapon of choice. Nothing epitomized the Iraq war's nature better than the insurgency's signature weapon. The IED resembles the insurrection itself: it takes many forms, it is difficult to identify, and its sophistication has grown tremendously since 2003.

The insurgency's strategy followed an old rationale. T.E. Lawrence, better known as Lawrence of Arabia, was a British military advisor to Arab tribes during the First World War. The Ottomans had occupied Medina. An Arab offensive in June 1916 on the city's Turkish garrisons was squashed, and the Arabs beaten back. Instead of repeating an open attack, Lawrence recommended attacking the Ottoman supply lines: the Hejaz railway, the Trans-Jordanian railway, and the Damascus-Aleppo connection. "Our ideal was to keep his railway just working, but only just, with the maximum of loss and discomfort to him."<sup>28</sup> Iraq's insurgents seem to have studied the Arab Revolt well. One of the coalition's most vulnerable points is supply, particularly fuel supply. In August 2005, for example, the Army 1st Corps Support Command's convoys suffered about 30 IED attacks per week. Support units are not trained and equipped for combat, which makes them easy and efficient targets. The long tail of small hits pushes up costs and depresses morale.

Bombs are hidden behind signs or guardrails, concealed under rocks or trash littered at the shoulders of roads all over Iraq. Some of the devices were hidden in the carcasses of dead

dogs, rotting in Baghdad's summer heat. Later, vehicle-borne IEDs were developed, with special drop-mechanisms in the car's belly - or the entire vehicle driven into the targeted convoy and exploded there. During the summer of 2003, the bomblets were still small, built out of mortar or single 152mm rounds. The insurgency's main targets were soft-skinned Humvees. As the coalition's armor improved, improvised mines grew bigger and more sophisticated. The firepower of multiple heavy artillery munitions, stacked anti-tank mines, or 500-pound Russian-made aircraft bombs was augmented with locally available chemicals. In 2006, army units were even losing large numbers of their once-invincible 63-ton, heavily armored combat vehicle, the M1A1 Abrams tank. One commander tells the story of a Bradley, a 35-ton fighting vehicle, which was literally blown into the air and broken in half by an IED; its crew was killed instantly. Not only is the bombs' power stunning, so is the insurgency's ability to innovate. IED trigger mechanisms are an example: Initially the mines were hardwired, and electronically ignited by an observer. GIs learned to spot the wires and to take out the operator at the end of the line. The insurgents then started to use cell phones, garage openers, remote controls for toy cars, or hand held radios. The army responded with Warlock, a frequency-jamming device. Insurgents reverted to hardwiring the bombs, or mechanical triggers such as pressure plates or even water hoses.

Ambushes are organized by cells. The insurgent network's overall structure is decentralized, which makes it difficult to penetrate small personalized groups of trusted activists and gather intelligence. A typical IED cell has 6 to 10 members with specific skills, innovative bomb builders, someone to transport and place it, a spotter to watch advancing patrols, a triggerman, and often a cameraman. (Many counterinsurgency missions in Iraq and Afghanistan equally embed a combat-camera team to counter the spin of those images<sup>29</sup>). More than 100 such cells reportedly operated in Mesopotamia in 2006. U.S. intelligence officers believe they receive some guidance from the larger insurgent networks and foreign terrorist organizations, such as Ansar al Sunna or al Qaeda in Iraq.<sup>30</sup> Their success is stunning. More than 45 percent of the more than 3,000 U.S. fatalities in Iraq have been caused by

roadside bombs; they have maimed or wounded more than 11,000 Americans. And their lethality is on the rise: of 100 recent fatalities, 67 were inflicted by IEDs.<sup>31</sup> The psychological impact on soldiers on patrol cannot be underestimated, even if they are not hit. The weapon's low price – in early 2006 the street price for a 152mm artillery round was \$100 to \$200 – its adaptability, and its simplicity likely make it a permanent feature of the battlefield of the future.

"We have a very adaptive enemy," said Brigadier General Joseph Votel, director of the Army's IED Task Force, in a closed door briefing on the threat situation to the Senate's Armed Services Committee on November 1, 2005.<sup>32</sup> Votel told the senators that this enemy is able to buy and learn to use the bombs' components via the internet. Senator John Warner, the committee's chairman, called it "astounding" that insurgents were able to make IEDs using information available from open sources and commercial, off-the-shelf technologies. Three months later, in February, the congressional research service published a report on the IED threat and available countermeasures. "The Iraqi insurgents make videos of exploding U.S. vehicles and dead Americans and distribute them over the Internet to win new supporters," it said. The videos demonstrate that the Americans can be hit, and that it is easy to do.<sup>33</sup> Mirroring the executive's as well as lawmakers' threat perception, the Pentagon's Joint IED-Defeat Organization, led by Montgomery Meigs, a retired four-star Army general, was outfitted with an impressively large budget of \$3 billion.

Cells advise their technical skills on the internet, with manuals outlining how to build explosives, as well as video documentation of attacks. "The Internet has changed the nature of warfare," said Lieutenant Colonel Shawn Weed, an Army intelligence officer based in Baghdad. "Someone can learn how to build a new bomb, plug the plans into the Internet and share that technology very quickly." This is an apt description of peer-to-peer networks, operating on the basis of open source knowledge, where the cells' activists are really co-developers. It's essentially like Wikipedia, just less easy to access.

Half a year later, on May 10, 2006, Lieutenant General Karl Eikenberry, then commander of the

Combined Forces Command in Afghanistan, was asked at a press conference whether the IED threat had migrated from Iraq to Afghanistan. Eikenberry said there was "no conclusive evidence" of a migration of foreign fighters. But he said that his command was observing a steady increase in the sophistication of roadside ambushes in both theaters. In the first eleven months of 2006, the number of IED attacks in Afghanistan rose to 1,297, up from 530 during the same period in 2005.<sup>34</sup> "These are the kinds of skills that, very frankly, in today's information age can be gleaned from the internet," Eikenberry said, "and be improved by a force that's operating against you over time as they continue to adapt their own tactics."

Not only have development cycles accelerated, various splinter groups loosely coupled their tactics. Generally technical superiority is seen as a battlefield advantage of modern armies. F-22s and B-52s certainly are farther advanced than AK47s or 152mm shells. But the complexity and costs of modern weapons systems are also a disadvantage; their coupling is tight and technologically complex. Once a force is equipped with blue force tracker and trained and set up to inter-operate jointly, it becomes very difficult to just plug in a partnering coalition force. Insurgencies do not face this problem. Barriers to entry, to use, and even to improved technology are low if the machinery is simple and standardized. Knowledge and techniques can easily be moved from one organization to another. RSS feeds are an example from today's internet. The technology is now a worldwide standard. IED tactics are an example of today's insurgency, and they are spreading as well. Locally from Shia dominated neighborhoods in Baghdad to Sunni quarters, and globally, from Chechnya or Iran to Iraq and from there to Afghanistan. Traditionally insurgent movements operated in their own countries, the FLN in Algeria, the IRA in Northern Ireland, the FARC in Columbia. Direct cooperation and the direct exchange of knowledge was very rare. Although some imitation of tactics took place before the internet, Web 2.0 has significantly increased the transnational character of guerrilla warfare.

The enemy's sheer tactical innovation speed outperforms the Army's traditional learning and adaptation routines. The first official doctrinal

document on how to react to the bombs, Field Manual Interim (FMI) 3-34.119, "IED Defeat," was published in September 2005, literally years after the bombs' debut in theater. Learning and adaptation cycles accelerate rapidly, as insurgents inadvertently operate according to the software industry's "release early, release often" paradigm. Innovative applications are considered imperfect by definition and are constantly being improved by their users, thereby pushing up innovation speed. "There is a constant cycle of new technologies, counter technologies, and counter-counter technologies," Weed pointed out in an interview with *Aviation Week & Space Technology*.<sup>35</sup> The Army recognized that the adversary's use of new technologies like digital cameras, mobile phones, and the internet accelerates this dynamic, and seems to heed junior officers' advice to mirror this structure. General Wallace, the head of TRADOC, highlighted the internet-based learning tools at the army's disposal and singled out SIPRNET, which offers a "collection of the current techniques being used to emplace and employ IEDs and indeed some techniques associated with how one might defeat those IEDs or at least identify them."<sup>36</sup> This thought has entered the most authoritative contemporary doctrinal document: "Learning organizations defeat insurgencies," Petraeus's counterinsurgency manual says, "bureaucratic hierarchies do not." Insurgent networks, however, have an organizational advantage over the hierarchical military they face.

## The enemy's new operating system

**T**he most spectacular internet-based propaganda operation in the history of terrorism was staged on May 11, 2004. A video showed Nicholas Berg, a civilian from West Chester, Pennsylvania, dressed in an orange jump suit, bound, sitting on the ground, masked men behind him. What follows is a gruesome beheading: Berg's startled expression, a knife sawing through his neck, screams, blood. The now-notorious five-and-a-half-minute video first appeared on a website of the militant group Muntada al-Ansar al-Islami, initially identified by a Reuters journalist. CNN and Fox News, among

others, immediately downloaded a copy of the video. Within less than 90 minutes, the file allegedly disappeared from the site; al-Jazeera was not able to obtain it from there. But the video spread to better-known forums and mirrored sites, and within 24 hours was downloaded approximately half a million times. The international media, talk shows, and editorial pages voiced outrage for weeks. President Bush condemned the beheading. The 26-year old American victim and the alleged perpetrator, Abu Musab al-Zarqawi, instantly became household names.

The execution illustrates a general trend: An interface between the mainstream "old media" and the radical "new media" is evolving. After a terrorist attack has been committed, several organizations and groups usually claim responsibility and "ownership." The problem for journalists is to recognize the authentic one. While the intelligence services assess the authenticity of these claims behind closed doors, the mainstream media's experts do so publicly. Yassin Musharbash, a Jordanian-born German journalist, is one of these experts. He writes for *Spiegel Online*, Germany's most widely read online paper. Musharbash gives an example of how the radicals have adapted to the need to be authentic. In summer 2005, al-Hisba was one of the preferred sites to find official communiqués. One day the site's operators demanded a registration including a valid email address. They even offered the possibility of accreditation for journalists. Eventually, in early 2006, al-Hisba published a list of all Western media organizations who used the site as a source for their reporting, complete with logos. It included the Associated Press, CNN, the Swiss News Agency, ABC News, and others.<sup>37</sup> The forum later even offered RSS feeds, so that communiqués from Iraq would be "pushed" directly onto journalists' desktops.

But a focus on propaganda, or "public affairs," as modern armies prefer, is too narrow. The overall number of radical websites has grown rapidly. Gabriel Weimann, a long-time Israeli observer of the field, counted 12 eight years ago. Today the number is hovering around 5,000.<sup>38</sup> In practice that figure is impossible to determine because many of the sites are too ephemeral to be indexed by search engines. While some radical websites strive for media interest

and cultivate their media readership, others have an extremely short life-span and try to avoid general publicity. This highlights the web's multiple uses: it facilitates not only public affairs or funding of radicalized organizations, but also recruitment, engineering, training, and syndication.

*Recruitment.* While recruitment of qualified soldiers is increasingly difficult for Western armies, the opposite is true for radicalized Islamist groups. The web's anonymity has stunning consequences: Junior officers discuss TTPs (tactics, training, and procedures) and may even counsel higher ranking fellow officers, and ordinary bloggers criticize and speak out despite oppressive regimes. Similar effects exist among radical groups: While in the real world very few people would admit membership in al Qaeda, in the jihadist internet, sympathizers abound, even if only a small fraction of online-jihadis have connections to the organization's hard core. Recruits can easily be contacted in chat-rooms or by email, even anonymously, or they might decide to take action independently. "The radicalization process is occurring more quickly, more widely and more anonymously in the Internet age," the U.S. government's National Intelligence Estimate 2006 concluded, "raising the likelihood of surprise attacks by unknown groups whose members and supporters may be difficult to pinpoint."<sup>39</sup>

*Engineering.* On September 1, 1992, Ahmed Ajaj, a Palestinian operative, was caught at New York's John F. Kennedy airport carrying two books of handwritten notes for explosives, six printed bomb-making manuals, and instructional videotapes. His faked Swedish visa had aroused suspicion. Ramsi Yousef, who traveled with Ajaj in the same plane, was temporarily arrested because he had no visa, and then released. In February 1993 Yousef, who learned his craft in an Afghan al Qaeda camp, carried out the World Trade Center bombings. Such a scenario would be highly unlikely today. Throughout the 1990s al Qaeda operatives wrote and used the *Encyclopedia of Jihad*, a multi-volume manual that covers explosives, small arms, grenades, mines, espionage, reconnaissance, sabotage, interrogation and counter-interrogation tactics, infiltration, tank ambushes, first aid, etc. Written probably in Afghanistan and Sudan, the

field manuals were initially handled restrictively and confidentially. After the 2001 offensive against the organization's strongholds in Afghanistan, the papers that once filled suitcases were first conserved on CD-roms, and probably in 2003 made available on the internet.<sup>40</sup> Today dozens of different versions, continually updated and improved, are on offer. Even films that explain the use of a suicide bomber's belt can be obtained. Not all peer-produced explosive user guides or poison recipes offer workable information, just as not all Wikipedia articles are of high quality. But even if sometimes flawed, open-source terrorism works.

*Training.* Ali Abdelsoud Mohammed was a worldly, charismatic al-Jihad activist, who in the early 1980s was sent to the United States by al-Zawahiri to infiltrate the CIA. He did not succeed in his original mission, but Mohammed married an American, enlisted in the U.S. Army, and was trained as a Special Forces trooper in Fort Bragg, North Carolina. In the late 1980s he traveled to Afghanistan and trained al Qaeda's far-flung recruits and fighters there (bin Laden supposedly took Mohammed's first class); later he even worked with Hezbollah in Lebanon.<sup>41</sup> Today, training manuals do not have to be smuggled out of the United States. The Islamist network attempted to replicate the Afghan or Sudanese training experience online. "Mu'askar al-Battar" is the best known training journal published online; it means the training-camp of the sword. Different issues feature discussions of light weapons, rocket-propelled grenades, and urban ambushes, as well as organizational tips on how to form a cell structure or increase physical fitness. "Oh Mujahid brother, in order to join the great training camps you don't have to travel to other lands," outlines the inaugural issue published in early 2004. "Alone, in your home or with a group of your brothers, you too can begin to execute the training program."<sup>42</sup> The objective was to delegate responsibility and initiative to entrepreneurs on lower levels, in what resembles a terrorist's crude version of *Auftragstaktik*. Each of the magazine's editions provided email addresses, encouraged submissions, and offered personal assistance if needed.

*Syndication.* Just how much command and control remains in the hands of top leaders is a matter open to dispute, even within the movement itself.

Bruce Hoffman argued that al Qaeda has both, a hard core able to retain command and control of larger operations in a top-down fashion, and a network of homegrown activists who take the initiative from the bottom up.<sup>43</sup> While the first view is controversial, the second is not: Google does not know how many entrepreneurs syndicate their services and integrate them into their businesses; the insurgency does not know how many individuals are using their tactics; and al Qaeda does not know how many observers became supporters or how many supporters took up arms and are combatants. The organization's boundaries are so flexible that Beam's notion of the "unity of purpose" is helpful, with the unifier being the jihadist ideology. The anonymous global community discusses the radical methods, its self-understanding, and its future strategic direction. Theological questions can be asked, and will be answered swiftly. Thanks to al Qaeda and the internet, the ancient Ibn Taimiyya of Damascus is today again one of the most widely read Arab religious scholars.<sup>44</sup> Today's jihad is fought with the methods and weapons of the 7th century and the 21st century simultaneously. Al Qaeda is also a giant global think tank, as indestructible as the internet itself.

## STRG, ALT AND DELETE?

**T**he trends described here have troubling consequences. They profoundly affect social networks, the centers of gravity in today's wars: within insurgent groups, within the increasingly complex setup of counterinsurgent actors, and, most centrally, with the neutral civilian population – both in theater and at home. The interactive media have, at first glance, two contradictory effects. They infuse both volatility and stability: On the one hand, they make public support in the metropolis for a protracted counterinsurgency campaign in far-away lands more volatile, even if the political stakes are high. A permanent stream of bad news and gruesome images from a protracted guerrilla campaign threatens to erode even strong public resolve. And the U.S. military in Iraq is one of the most isolated occupiers in history. There are no bars, no suqs, no brothels – mostly for cultural and security reasons, but technology

adds to the problem: a chatting, cell-phoning, photographing, and video-blogging occupying force maintains tight social connections to its distant home communities, while local ties fail to develop. On the other hand, though, the new media stabilize the insurgency and militant movements. Even if the local population's support for the insurrection is waning as a result of a successful counterinsurgency campaign, radicals are still able to make instant use of propaganda-driven operations to gain moral, financial, organizational, and operational support from global audiences. America faces some of the most adaptive and entrepreneurial adversaries it has ever encountered militarily

What, then, can and what cannot be done? First the no-goes. It is neither possible nor desirable to shut down internet in theatre, to black out mobile phone networks, or to strip soldiers of their civilian communication devices. Such methods are essentially illiberal strategies. They send a wrong message, and they are economically and socially unsustainable in a protracted counterinsurgency campaign. More important, however, they ignore the new media's positive potential.

For governments, perception management, or public diplomacy, has become infinitely more complex. But simultaneously its prospects have never been better. The use of government-controlled old media, such as the State Department's Cold War-style TV channels and foreign language radio services is, for the most part, a waste of resources: more than \$640 million are appropriated for "international broadcasting operations" for 2007. Such broadcasts are stuck in the old, one-way-street paradigm, and cannot compete for credibility in an increasingly crowded media market in the Middle East. Instead, programs that create durable social contacts and linguistic skills through dialogue should receive more support, beyond the traditional educational exchange schemes. Taxpayers' money should instead be used to aggressively promote internet and mobile phone penetration in conflict-ridden areas, thus creating a platform for engagement of civil society. Finally, governments should appreciate that the enemy is forced to communicate openly, and adapt its intelligence services accordingly; they need to be more open to recruits from minority groups with the appropriate linguistic

and IT skills.

For the military, the consequences are even more significant. As long as the right ingredients are available – frustration, ideology, and the know-how to take action – militant Islamic fundamentalism will be “just another feature of the battlefield terrain.” The expectation to win, consequently, should be replaced by a more humble hope to be successful; the objective of extinguishing terrorism should be abandoned. But the repercussions are not only conceptual, they are also organizational: The U.S. military is culturally disposed to destroy the enemy rather than to create stability in an alien environment. To change this, career incentives and promotions schemes should be reorganized to place more value on the specific skill-set required of a successful counterinsurgent. The insurgent is not hampered by a bureaucratic hierarchy, so the counterinsurgent should be able to fast-track the most talented individuals into leadership positions. The “I had 500 cups of tea with the locals, and now I’m out” problem also needs to be addressed. The practice of rotating an entire unit out of an area after its commanders built rapport with civilian leaders, and thereby cutting established social contacts, should be overhauled. Unit cohesion should be weighed against social cohesion with civilians in the war zone.

Development agencies should face the fact that they are engaged in a counterinsurgency campaign if they operate in Afghanistan or Iraq. Just as soldiers do “social work,” in Galula’s words, external nongovernmental actors do “military work”: if their performance and their projects are successful, international organizations and NGOs not only create stability, they undermine trust and undercut social networks between the insurgency and the civilian population. So it should come as no surprise that aid workers are often seen as targets by the insurgents. Here, again, the new media may alter the rules of the game in the future. Both long distances between villages, such as in Afghanistan, as well as security threats in an urban environment, such as in today’s Baghdad, limit the mobility of civilians. The interactive media could in future – given the necessary preconditions – be used for schooling, education, or political participation, and thereby limit the insurgents’ impact on the

population. In many areas this is still unrealistic today, but it will not be so in the future.

Finally the mainstream media should welcome the trends described here. The new media are a new source for journalists and editors. Blogs give the print media an alternative to quoting officials and insert fresh perspectives, particularly if the security situation in a war zone makes free reporting difficult. Independent specialists and experts could validate the authenticity of blogs, even if their authors remain anonymous. It is accepted practice to quote any Washingtonian "senior official" without identifying him or her publicly; a similar convention should be developed for civilians in war zones. The risk they take is much higher than that of a White House leaker. Even anonymous interviews via Skype may become an option.

The web's emerging organizational patterns have not diminished the significance of old, traditional businesses and their products. But management, communication, supply-chains, R&D, production, administration, marketing, customer relations, and competition itself are subject to fundamental changes – changes that come with both great risks and great opportunities. The same applies to the management of violence.

---

<sup>1</sup> Greg Grant, "Behind the Bomb Makers," *Aviation Week & Space Technology* (January 30, 2006).

<sup>2</sup> Seema Mehta, "Grief, comfort meet on MySpace," *Los Angeles Times* (January 24, 2007).

<sup>3</sup> The term peer-production was first introduced in a now classic article by Yale University's Yochai Benkler, "Coase's Penguin, or Linux and the Nature of the Firm," *Yale Law Journal* 112:3 (December 2002); see also Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press, 2006).

<sup>4</sup> Doug Kaye, *Loosely Coupled: The Missing Pieces of Web Services* (RDS Press, 2003), 131. The concept was originally introduced by the sociologist Karl Weick in 1976, who applied it to educational organization. Karl E Weick, "Educational Organizations as Loosely Coupled Systems," *Administrative Science Quarterly* 21:1 (1976).

<sup>5</sup> The term was coined by *Wired's* Chris Anderson. His argument is that the total commercial volume of low-popularity items can beat the volume of high-popularity items – a logic that is easily transferable to an insurgency's low-intensity attacks and the occupier's high-intensity response. Chris Anderson, *The Long Tail: Why the Future of Business Is Selling Less of More* (Hyperion,

---

2006).

<sup>6</sup> David Kilcullen, "Twenty-Eight Articles. Fundamentals of Company-level Counterinsurgency," *Military Review* (March-April 2006).

<sup>7</sup> C.E. Caldwell, *Small Wars: Their Principles and Practice* (University of Nebraska Press, 1896, 1996).

<sup>8</sup> T.E. Lawrence, "The 27 Articles," *Arab Bulletin* (August 20, 1917); T.E. Lawrence, *Seven Pillars of Wisdom* (London: Bernard Shaw, 1926).

<sup>9</sup> Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-keeping* (London: Faber, 1971).

<sup>10</sup> Roger Trinquier, *La Guerre moderne* (Paris: La Table ronde, 1961); David Galula, *Counterinsurgency Warfare: Theory and Practice* (Praeger, 1963); David Galula, *Pacification in Algeria 1956-1958, MG-478-1* (Rand Corporation, 1963, 2006).

<sup>11</sup> Lawrence Wright, *The Looming Tower. Al-Qaeda and the Road to 9/11* (Alfred A. Knopf, 2006).

<sup>12</sup> Mao Zedong, *On Guerrilla Warfare* (London: Cassell, 1965), 93.

<sup>13</sup> The idea of a "unity of purpose" was brought up by a right-wing American supremacist, Louis Beam – not because such an organization is more practical, but less vulnerable. Kilcullen prefers a "common problem definition." David Kilcullen, "Counter-Insurgency Redux," *Survival* 48:4 (Winter 2006); see also Louis Beam, "Leaderless Resistance," *Seditionist* 12 (February 1992).

<sup>14</sup> Robert R Tomes, "Relearning Counterinsurgency Warfare", *Parameters* (Spring 2004).

<sup>15</sup> Audrey K Cronin, "Cyber-Mobilization: The New Levée en Masse" *Parameters* (Summer 2006).

<sup>16</sup> Donatella Lorch, quoted in Thomas Rid, *War and Media Operations. The US Military and the Press from Vietnam to Iraq*, (London: Routledge, 2007).

<sup>17</sup> Charles W. Ricks, *The Military-News Media Relationship: Thinking Forward* (Army War College, 1993).

<sup>18</sup> John Hockenberry, "The Blogs of War," *Wired* (August 13, 2005).

<sup>19</sup> Peter Maass, "Salam Pax is Real," *Slate* (June 2, 2003).

<sup>20</sup> Dan Baum, "What the Generals Don't Know," *New Yorker* (January 17, 2005).

<sup>21</sup> Thomas E. Ricks, "Soldiers Record Lessons From Iraq", *Washington Post* (February 8, 2004)

<sup>22</sup> Pete Kilner, interview with author (January 27, 2007).

<sup>23</sup> Sandra I. Erwin, "Washington Pulse," *National Defense* 90:627 (February 2006).

<sup>24</sup> Andrew P. Schilling, "Peers," *Marine Corps Gazette* 90:5 (May 31, 2006).

<sup>25</sup> Ron Dysvick, CEO of Triple-I, quoted in Greg Slabodkin, "Army Lessons Learned," *Federal Computer Week* (July 17, 2006).

<sup>26</sup> U.S. Army/U.S. Marine Corps, *Counterinsurgency, FM 3-24* (December 2006).

<sup>27</sup> Michael Gordon and Bernard Trainor, *Cobra II. The Inside Story of the Invasion and Occupation of Iraq* (Atlantic Books, 2006); Thomas E. Ricks, *Fiasco. The American Military Adventure in Iraq* (Penguin, 2006); Rajiv Chandrasekaran, *Imperial Life in the Emerald City* (Knopf, 2006).

<sup>28</sup> T.E. Lawrence, "The Evolution of a Revolt," *Army Quarterly and Defence Journal* (October 1920).

<sup>29</sup> Cronin, "Cyber-Mobilization: The New Levée en Masse."

- 
- <sup>30</sup> Grant, "Behind the Bomb Makers."
- <sup>31</sup> Brad Knickerbocker, "Relentless toll to US troops of roadside bombs," *Christian Science Monitor* (January 2, 2007).
- <sup>32</sup> *Defense Daily* 228:20 (November 2, 2005).
- <sup>33</sup> Clay Wilson, *Improvised Explosive Devices (IEDs) in Iraq: Effects and Countermeasures* (Congressional Research Service, 2006), 1.
- <sup>34</sup> Anthony Cordesman, "One War We Still Can Win," *New York Times* (December 13, 2006).
- <sup>35</sup> Grant, "Behind the Bomb Makers."
- <sup>36</sup> William Wallace, quoted in Ann Roosevelt, "Army TRADOC works IED issues," *Defense Daily* 228:46 (December 16, 2005).
- <sup>37</sup> Yassin Musharbash, *Die neue al-Qaida. Innenansichten eines lernenden Terrornetzwerks* (Köln: Kiepenheuer & Witsch, 2006), 111.
- <sup>38</sup> Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (United States Institute of Peace), 2006.
- <sup>39</sup> U.S. Director of National Intelligence, "Trends in Global Terrorism: Implications for the United States," National Intelligence Estimate (April 2006).
- <sup>40</sup> Musharbash, *Die neue al-Qaida*.
- <sup>41</sup> Wright, *The Looming Tower*, 184-188.
- <sup>42</sup> MEMRI, Dispatch 637 (January 6, 2004).
- <sup>43</sup> Bruce Hoffman, "From the War on Terror to Global Counterinsurgency," *Current History* (December 2006).
- <sup>44</sup> William McCants, *The Militant Ideology Atlas*, Combating Terrorism Center (U.S. Military Academy, November 2006).

---

Thomas Rid is a Tapir Fellow at the Institut français des relations internationales (Ifri) in Paris, at Johns Hopkins University's School for Advanced International Studies (SAIS), and at the Rand Corporation. Previously he worked at the German government's foreign policy think tank Stiftung Wissenschaft und Politik and the American Academy in Berlin. He is author of *War and Media Operations. The U.S. Military and the Press from Vietnam to Iraq* (Routledge, 2007). Christofer Burger's inspiration, Marc Hecker's counsel, and Pete Kilner's fact checking, significantly improved the text. The author thanks them.