

The Secret Posse

Behind the veil of national security, information warfare is eclipsing the difference between military and domestic affairs.

By Geoffrey Klingsporn

IMAGINE THAT AN AMERICAN MILITARY computer network is under attack. The enemies are unknown, but they seem to be operating from a cybercafe in the Middle East, and they have gained access to classified data. Following standard procedure, system administrators respond with "hack-back" maneuvers to disable the intruders' equipment. Only later does it become apparent that the offending machines were in the United States.

Meanwhile, on the ground in Iraq, a U. S. Army brigade's information officer cultivates friendly relations with American journalists in his area. He gives the reporters information on upcoming operations and, in return, they promise to give him the chance to respond in advance to any negative stories they plan to file.

What do these scenarios have in common? Under current military policy, both fall under the heading of "Information Operations," officially defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems." And in both cases, the "actions" are aimed at targets inside America's borders.

Every U.S. soldier swears to "support and defend the Constitution of the United States against all enemies, foreign and domestic." But in the age of information warfare—the use of computers and information networks as military weapons—the distinction between an enemy at home and one abroad has grown blurry, and that should worry every American.

The law that, in effect, prevents the Army from acting as a national police force is the Posse Comitatus Act, an 1878 statute that prohibits law enforcement officers from using military personnel as a posse comitatus—Latin for "power of the county" or, in the vernacular of the Old West, a "posse"—to enforce domestic law, except with the express authorization of the president or Congress. As its detractors are quick to point out, the law was enacted for the racist purpose of preventing federal soldiers from helping black Americans by enforcing voting laws in the post-Civil War South. But such disreputable origins should not obscure the significance of the dangers from which the act can shield us.

"The use of military forces to seize civilians," wrote the U.S. Court of Appeals for the Eighth Circuit, "can expose civilian government to the threat of military rule and the suspension of constitutional liberties," and can chill free speech and other fundamental rights, creating the atmosphere of an enemy occupation. In one notable instance, two protestors relied on the act to defend themselves against charges that they had

obstructed justice when they tried to get supplies to Native Americans who had seized Wounded Knee, S.D., in 1973. A federal judge dismissed the charges because the arresting officers had violated the act by receiving the Army's help. But the potential perils of military intrusion are so widely acknowledged that, in 127 years, it has rarely been necessary to invoke the act's protections.

Since the 1980s, though, the statute has been weakened by laws that allow the military to help address the problems of drug trafficking, natural disasters, and terrorist attacks. It is now routine for soldiers and sailors to help state and local police with training, equipment, and logistics; to detect and monitor suspected smugglers; and to keep order in disaster areas. Critics have objected on practical and constitutional grounds to the military's increasing involvement in such activities, arguing that soldiers are neither trained nor equipped for law enforcement, and that the growing list of new duties has stretched the military thin. But the courts generally have ruled that it is well within the discretion of the president and Congress to allow the military to help in nonmilitary situations, including cases of terrorism. In 1988, a federal district judge in Washington, D.C., ruled that the Posse Comitatus Act was not violated when the FBI used the Navy to help capture a suspected terrorist in international waters and transport him to the United States.

Still, the D.C. judge reaffirmed that "limiting military involvement in civilian affairs is basic to our system of government." Then came the attacks of September 11, the war on terror, and further erosion of posse comitatus as a matter of law. In the face of terrorism, it is difficult to defend an old and rarely used statute already riddled with exceptions. And strategically, it seems unwise to hinder law enforcement and military operations with further restrictions on cooperation and information sharing between them.

But the protection that the act offers is even more important in an age when most Americans seem to welcome rather than fear military flyovers at the Super Bowl and National Guard members toting M-16s at airports. While keen about developing a reliable army and navy, the nation's founders insisted on a strong, civilian government that would protect democracy by reining in the military's authoritarian nature. The Posse Comitatus Act, in effect, reinforced the founders' intentions by curbing military power, which government critics believed had grown excessive in the Civil War's aftermath.

Since September 11, the act's principles seem to have muted calls for more military involvement in domestic security. In July 2002, for example, Sen. Joseph Biden, the Democrat from Delaware, proposed that soldiers be allowed to arrest suspected terrorists in the United States and "shoot to kill" anyone possessing a "terrorist weapon." Senior military officers echoed Biden's proposal, but Director (later Secretary) of Homeland Security Tom Ridge later squelched the idea, saying it "generally goes against our instincts as a country to empower the military with the ability to arrest." Missing entirely from these exchanges, however, has been any mention that information warfare ignores the distinction between foreign and domestic threats, a difference fundamental to the Posse Comitatus Act.

INFORMATION WARFARE EVOKES IMAGES FROM SCIENCE FICTION and inspires rhetoric that exaggerates the capabilities of current technology. But that form of warfare is also a bureaucratic, budgetary, and battlefield reality that has become integral to the Defense Department's view of the world. It is a tactic that has been developed over the last few decades in response to terrorism, drug smuggling, attacks on computer networks, and other nontraditional forms of warfare. Information warfare also marks a dramatic change in what the government perceives as a threat.

The ideas behind this tactic began to develop in the 1980s as defense experts articulated fears about new dangers for the nation. The experts warned of "asymmetric threats" and, more lyrically, attacks at the nation's "center of gravity," a term that nicely captures the sense of the United States as a gigantic but lumbering superpower. Enemies might come from any part of the world, including from within this country, and the most dangerous among them would not be other nations but rather nonstate actors, small groups, or even individuals.

In 1996, the Clinton Administration's national-security strategy identified a new "transnational" and "terrorist" class of "problems which once seemed quite distant." America's national enemies had been joined by criminal groups representing no particular state, who were able, through sophisticated organization and technology, to disregard national boundaries. A military task force suggested that nonstate actors could be a clear and present danger.

Under the Bush Administration, information warfare is on the verge of eliminating any distinction between domestic and foreign enemies. The 2003 National Strategy to Secure Cyberspace admits that "the speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all." Current Defense Department doctrine compounds the problem by putting everything from public affairs to attacks on a computer network under the same heading of "Information Operations." In Afghanistan, military officers treat as similar threats hostile artillery and hostile information—in military jargon, "lethal and nonlethal fires." Journalists, and through them the American public, are often among the targets the officers seek to combat.

The rise of information warfare has outpaced the development of laws to deal with it. In its chapter on information warfare, the Army's legal manual makes no mention of the principles behind the Posse Comitatus Act or of limits on using information warfare in domestic operations.

As the distinction is erased between foreign foe and domestic opponent, cyberterrorist and cybercriminal, the relationship between this country's citizens and their military is being turned upside down. It's a well-intentioned response to today's geopolitical dangers, but the silent repeal of the Posse Comitatus Act is a choice that many Americans would resist making—if they knew they were making it.