In any war, surveillance of the enemy is critical. Today, in the eyes of at least some Americans, surveillance itself has become the enemy.

It was not always so. As any intelligence maven knows, some of the heroes of World War II were eavesdroppers, not soldiers. They were quiet, wonkish men, like those who monitored and deciphered Nazi communications about German battle plans at Bletchley Park, an estate 50 miles northwest of London. Their super-secret operation employed thousands of people who listened to 226 radio frequencies for dot-and-dash messages and passed them to ingenious code-breakers. The results were kept on 5-by-7 inch cards in shoe box-shaped containers.

Who are our masters of surveillance today? Most are located at the National Security Agency, the giant "Crypto City" complex located off Interstate 95 between Washington and Baltimore. The agency vacuums up 650 million intercepts a day -- called signals intelligence, or sigint -- from satellites, ground stations, aircraft, ships and submarines around the world. And it hunts for patterns that might lend seemingly ordinary words significance in the war on terrorism.

But the agency and its experts are not being hailed as heroes right now. The NSA, so secretive that its letters are commonly said to stand for "No Such Agency," has been uncomfortably in the limelight in recent weeks after the New York Times revealed that as the result of a presidential order, the agency has been monitoring thousands of Americans over the phone and by e-mail without court authorization.

As the controversy over the legality and propriety of domestic surveillance by the National Security Agency rages on, one question has not been adequately addressed: Is the NSA's approach really the best way of tracking terrorists? While there's no question that the NSA's covert move into domestic surveillance raises serious legal and ethical issues, the equally important and less examined question is whether -- more than four years after 9/11 -- the agency's methods are suited to tracking the jihadists.

The difference between Bletchley Park and Crypto City has as much to do with the very different nature of their tasks as with the way they are viewed. By today's standards, the mission at Bletchley Park was well-defined. The targets of the surveillance were clear: the German high command and intelligence service. The signals collectors had a good fix on what communications to monitor. The greatest challenge lay in breaking the extremely complex Enigma code.

By contrast, the NSA conducts broad-based surveillance indiscriminately over communications lines that few bad guys even use any longer. "Big Noddy," as those in the know call the NSA's vast "Ear in the Sky,"
has capabilities that dwarf the Bletchley Park World War II enterprise, but it isn't picking up much because the smartest terrorist groups have long since stopped talking about their plans over cell phones or land lines -- or to the extent they do, it's probably to plant disinformation. Today the challenge isn't decoding an intercepted message from a known enemy; instead it's figuring out what is and isn't a message and who the enemy is.

The NSA was designed to monitor a relatively contained number of official communications pipelines in nation-states -- for example, microwave transmissions from Moscow to an intercontinental ballistic missile (ICBM) base in Siberia. But as Michael Hayden, then NSA director, told me in an interview in late 2002: "We've gone from chasing the telecommunications structure of a slow-moving, technologically inferior, resource-poor nation-state -- and we could do that pretty well -- to chasing a communications structure in which an al Qaeda member can go into a storefront in Istanbul and buy for $100 a communications device that is absolutely cutting edge, and for which he has had to make no investment for development."

The result is that the NSA is overwhelmed by millions of phone calls and e-mail contacts that it simply can't digest. And it's not just a question of finding the needle in the haystack; today's surveillance professionals aren't sure what the needle looks like. The agency has adjusted, but it continues to perform what some experts consider to be primitive, broad-based techniques, like random keyword searches on the Web for Islamist tag lines. As a December 2002 report by the Senate Select Intelligence Committee noted, "Only a tiny fraction of the daily intercepts are actually ever reviewed by humans, and much of what is collected gets lost in the deluge of data."

Moreover, communications between terrorist groups today, says one intelligence official, is either "air-gapped" -- in which a document or computer disk is hand-delivered by messenger (as was seen in the letters allegedly exchanged between al Qaeda chieftain Ayman Zawahiri and Iraqi insurgent leader Abu Musab Zarqawi) -- or it occurs through Web sites. Some intelligence experts who are critical of NSA's efforts, like John Arquilla of the Naval Postgraduate School in Monterey, Calif., a sometime Pentagon consultant, say the real problem is that the agency is still pursuing a Cold War-era strategy.

What the NSA really needs to do, say Arquilla and others, is to build a new Bletchley Park. Just as Bletchley attracted Alan Turing, inventor of the modern computer, the NSA needs to summon the Turings of our day -- mainly computer hackers -- to snare al Qaeda and other terrorists at the only place they still communicate electronically, on Web sites. An added benefit, Arquilla adds, is that "if we went the route of a much greater emphasis of intelligence collection on the Web and Net, we would learn a lot more and intrude less on civil liberties."

Bruce Hoffman, a terrorism expert at the Rand Corp., notes that most of the major breakthroughs against al Qaeda-linked plots in recent years have shown that the terrorists, wary of phone monitoring, are communicating through couriers on the ground and coordinating plots on the Web. When Muhammad Naeem Noor Khan, a protege of Khalid Sheikh Mohammed, was arrested in July 2004, his laptop contained plans for simultaneous attacks on London and New York that were to have been transmitted electronically. Today, adds Hoffman, the most sophisticated terrorists have learned to evade the NSA altogether. "They keep their messages in a draft file on a Web site, then give someone the password and user name to get in. The NSA can't track that, because it's stationary."

Bush administration officials are now casting the war on terrorism as a fight against al Qaeda's plans to reestablish a "caliphate" across the Islamic world, referring to the Muslim empire of centuries past. Some experts scoff at such Islamist ambitions. But to the extent the dreams of a caliphate are being discussed by
extremist Muslim groups, this is occurring mainly on Internet Web sites, experts say. "The Internet is the key issue," Gilles Kepel, a prominent Arabist and a professor at the Institut d'Etudes Politiques in Paris, told the New Yorker in 2004. "It allows the propagation of a universal norm, with an Internet sharia and fatwa system."

Even loyalists of the NSA concede that Crypto City is in some respects a dinosaur -- and a very expensive one. While its budget numbers remain "black," or classified, one Defense Department contractor who is privy to the budget data says that traditional NSA tracking consumes much of the intelligence community's budget of roughly $40 billion a year, while Web-focused efforts consume only a small fraction of that. Finding and getting into these sites is difficult, but efforts did uncover (and ultimately destroyed) two terrorist groups in sub-Saharan Africa.

Ignoring Web sites can be costly. After the March 11, 2004 train bombings in Madrid just before Spanish elections, a Norwegian think tank, Forsvarets Forskningsinstitutt, discovered an Islamist strategy paper on an obscure Web site that might have signaled the attacks ahead of time. The document said, "It is necessary to make utmost use of the upcoming general election in Spain in March next year. We think that the Spanish government could not tolerate more than two, maximum three blows, after which it will have to withdraw [troops from Iraq] as a result of popular pressure."

NSA and other intelligence officials say that they are doing their best to cope and that the public misunderstands what the agency does. At a news briefing in late December after the domestic surveillance story broke, Hayden -- who is now deputy intelligence director but was head of the NSA when Bush authorized it to perform domestic surveillance -- insisted that his agency was carefully targeting certain conversations based on intelligence. "What we are talking about here are communications we have every reason to believe are al Qaeda communications, one end of which is in the United States," he said. "We can't waste resources on targets that simply don't provide valuable information."

Other NSA officials insist they are moving to reorient the whole agency. According to an NSA spokeswoman, who in the secretive spirit of the agency would speak only on condition that she not be identified, the agency began a campaign in 2004 to recruit about 7,500 new employees over the next five years. Among them will be close to 350 computer scientists, along with engineers, language analysts and a slew of new signals analysts, cryptologists and mathematicians. But, Arquilla says, many of the best people, some of whom are illicit hackers, simply cannot be vetted through today's security clearance process.

As America's intelligence network reorganizes -- Bush last year created a new director of national intelligence -- some intelligence experts worry that these efforts are still marginal. The kind of fundamental rethinking that would rechannel some of those billions of dollars from the NSA's global surveillance into more human intelligence and Internet surveillance is not taking place.

It may be possible for the NSA to conduct its massive surveillance legally, but solving the civil liberties issue is only half the agency's problem. Robert Holliday, a U.S. Customs expert who developed terrorist-identifying software that's now widely used, says the bad guys still have the edge when it comes to communicating in anonymity and secrecy. "I'm not going to worry about Big Brother," says Holliday. "There's just too much data to track out there." And America needs to find a better way to do it.

Author's e-mail: michael.hirsh@newsweek.com

Michael Hirsh covers foreign affairs for Newsweek and is the author of "At War With Ourselves" (Oxford
University).