US military blocks soldiers' access to blogs, popular social sites

Naomi Spencer
21 May 2007

The US Department of Defense issued regulations April 19 severely curtailing the use of the Internet by military personnel, contractors, and their families. As of May 14, the Pentagon has blocked use of public weblogs, forums, video hosting and social sites on military-run networks, citing bandwidth limits and security.

Blocked from military networks is the enormously popular social networking site MySpace, which many deployed soldiers used to keep in touch with family and friends. Also blocked is the video-sharing site YouTube, where soldiers had been uploading unauthorized original footage of combat, other troop activity, and daily life in Iraq.

In addition, 11 other sites frequented by troops have been blocked, including the video sites ifilm, FileCabi, and Metacafe; photo-sharing site Photobucket; Internet music and broadcasting sites Live365, MTV, Pandora, 1.fm; and the social sites BlackPlanet and hi5.

Defense officials are increasingly concerned about the growth of anti-war sentiment within the military, as well as the possibility that atrocities committed by US troops may be exposed. As public outrage at the leaked photographs of prisoner abuse from Abu Ghraib demonstrated, the US administration and military leaders have every reason to want control over what information comes out of occupied Iraq.

In addition, the Army revised its Operations Security (OPSEC) regulations to curb information from military operations. The OPSEC regulations (available in pdf via *Wired News*) present the social networking access primarily as a security rather than technological issue.

"In recent years," the document states, "the Internet has become an ever-greater source of open source information for adversaries of the US, websites in particular, especially personal websites of individual Soldiers (to include web logs or "blogs"), are a potentially significant vulnerability."

In seeking to justify curtailing blog activity, the document sounds an ominous tone for civilian as well as military information flows. "Because the US is a free and open society, information is readily available and easy to access. Adversaries are exploiting this vulnerability by aggressively reading open source and unclassified material about the US Army."

Open source material, the regulations explain, make up "80 percent of the adversary's intelligence needs" and includes "photographs, newspapers, magazine advertisements, government and trade publications, contract specifications, congressional hearings, computers and other public media." It also includes "public presentations, news releases from units or installations, organizational newsletters (both for official organizations and unofficial organizations, such as alumni or spouse support groups), and direct observation." In other words, every public statement about the war is potential intelligence for Al Qaeda, according to the military.

The restrictions are far more sweeping than the military-wide blocking of public websites. Under the Army regulations, soldiers are required to consult with their immediate supervisors and OPSEC officers prior to publishing or posting any information in a forum, any website, or in articles, e-mails, blogs, and even written letters. Material considered sensitive or critical includes information about troop casualties, battle scenes and Improvised Explosive Device (IED) strikes, and details about military outposts.

This regulation applies not only to "military and civilian personnel of the Active Army, the Army National Guard of the United States/Army National Guard, the United States Army Reserve and related activities of those organizations," but also to civilian contractors and family members back in the United States. Family members are expected to follow the regulations as well, to "protect critical and sensitive information."

Soldiers who publish material deemed "critical" or "sensitive" to security will be subject to military discipline, including court martial under the Uniform Code of Military Justice. For contractors and, potentially, family members, whom the military defines as part of the "Total Army," "Personnel not subject to the UCMJ who fail to protect

critical and sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action."

Military spokespersons, downplaying the severity of these restrictions, have insisted the website blocks are not a form of censorship but rather a matter of freeing up the network from what they characterized as "recreational traffic." At a press conference May 17, the *Washington* Post reported, the vice director of the Defense Information Systems Agency, Rear Admiral Elizabeth Hight, told reporters that the military "cannot accommodate the growth in bandwidth demands from these newer technologies." Asked whether the bandwidth had been compromised before, she commented that the block was "proactive."

The official talking points are bogus on a number of levels. Most obvious are the exceptions the military makes for higher-ranking officials, who may request exemptions from the policy. Secondly, the military runs ads on the social networking and video sites in order to draw in recruits. According to Rear Admiral Hight, recruiters have already been granted a waiver from the block.

Moreover, only days before the block policy was drafted, the Pentagon launched its own Multi-National Force Iraq channel on YouTube, which purports to "give viewers around the world a 'boots on the ground' perspective of Operation Iraqi Freedom from those who are fighting it," while editing videos for "time, security reasons, and/or overly disturbing or offensive images."

Material withheld or edited out includes "profanity; sexual content; overly graphic, disturbing or offensive material;" and "footage that mocks Coalition Forces, Iraqi Security Forces or the citizens of Iraq."

The Google corporation subsidiary YouTube, which already voluntarily removes graphic footage of violence committed against or by US troops, has announced that it will work with the military to be exempted from the block.

Also this month, the Iraqi government implemented a ban on the filming of bombing scenes by news photographers and camera operators. Effectively, unauthorized videos uploaded to Internet sites could become the only way such events become known to the public.

Military officials have said that troops are still allowed to access the blocked sites on outside networks if they have personal computers or are able to visit Internet cafes. But in many areas where US military personnel are stationed, connections outside of Defense Department networks are scarce or nonexistent, and personnel stationed on ships or otherwise physically remote areas cannot regularly reach other networks. In some regions of Iraq, troops may access the sites at Internet cafes hosted by a non-governmental vendor.

With regard to the claim that bandwidth faces overuse, there are longstanding Internet mechanisms, known as Quality of Service guarantees, which can automatically prioritize the type and size of data flows in order to optimize the efficiency of traffic on a limited network. The Department of Defense, which maintains more than 15,000 networks accommodating 5 million computers, could easily implement a system whereby data requests such as video uploads would receive lower priority on the networks.

In reality, the military has long been concerned by the flow of unauthorized material on the Internet and is taking this "proactive" step in preparation for popular backlash and escalation of the war. Over the past decade, numerous steps have been taken by the Pentagon to control information at its source, particularly in Middle East operations, such as attaching public affairs officers to units and carefully vetting troops who appear with visiting politicians.

The Pentagon has also managed media coverage by "embedding" journalists who agree to abide by military guidelines. But even the number of embedded journalists has been drastically cut over the past four years, from 770 at the time of invasion to *nine* as of September 2006. Four of the remaining nine are part of the Defense Department's own media outlets, *Stars and Stripes* and *Armed Forces Network.*

In 2005, commanders in Iraq told military personnel who kept blogs that they had to register their sites with their superior officers. The Army imposed additional restrictions on bloggers later that year by ordering that soldiers be granted approval from their commanders before posting. The following year, an order from the Joint Chiefs and Secretary of Defense stated that no information could be placed on any website prior to approval by Public Affairs officers.

Last October, the Army announced it had assembled a "Web Risk Assessment Cell" for the purpose of further monitoring soldiers' blogs, post-commander approval. Not surprisingly, the number of soldier-administrated blogs and online journals dropped significantly as a result of the regulations, particularly those presenting a critical or negative perspective on the Bush administration and the war.