The Internet and the Iraq Conflict

Dorothy E. Denning

July 2008

On blogs and Web sites, by e-mail and video, the Iraq war is fought on the Internet


In recent years, the Internet has come to play a part in every major conflict, for example, Kosovo in 1999, the ongoing Israeli-Palestinian conflict, particularly since the second Intifada in 2000, and now Iraq. While the net’s role in the Iraq conflict may seem insignificant compared to events on the ground, it cannot be ignored. At the very least, it has affected support for the war and for al-Qa’ida’s insurgency, both within Iraq and globally.

This chapter examines how the Internet has been and continues to be used in the Iraq conflict. This use is manifest in a range of activity from the dissemination of information to cyber attacks. The chapter describes who is engaging in these activities and some of the effects. It also considers how the Internet might be used more effectively to counter al-Qa’ida in Iraq and the al-Qa’ida/global Salafi jihad social movement. First, however, the chapter briefly summarizes the state of the Internet.

The Internet

According to Internet World Stats, approximately 1.3 billion people, about 20% of the world’s population, were connected to the Internet as of December 2007.¹
Connectivity varies by region, with North America having the highest penetration rate at 71%, compared with Africa’s lowest at 5%. The Middle East, at 17%, is a little below average, but some countries within the region, including Iraq, are well below that. Indeed, the data for Iraq shows only 36,000 users, or 0.1% of the population connected. This estimate was made in October 2005, however, so the number has likely increased, especially considering that the Internet population for the Middle East as a whole grew by 920% from 2000 to 2007. In addition, the data for Iraq might not take into account all of the Iraqis who access the Internet through cyber cafés. In 2004, Baghdad alone was reported to have 150.2

With such a low penetration rate within Iraq, it might seem that the Internet would have little impact on Iraqis. Yet, this is not the case. One reason is that information can jump media. For example, information that is distributed through the Internet can be picked up by Iraqi television, radio, and news media, and then passed along to the Iraqi public through the local media. In addition, Iraqis who are connected to the net can share information they acquire online with friends and family through face-to-face conversations.

Another reason why Iraqis are not immune to Internet activities is that information disseminated on the Internet can influence the decisions and actions of anyone exposed to it, which can in turn impact the Iraqi population. This information could originate from Iraqis, coalition forces, reporters and visitors to Iraq, foreign militants in Iraq, and other parties with Internet access. Al-Qa’ida in Iraq, for example, uses the Internet to help bring foreign fighters to Iraq, where they then kill Iraqis as well as coalition forces.
With that background, we now examine specific ways in which the Internet has been employed in the Iraq conflict. The discussion focuses on activities that relate to the initial US-Iraq interstate war and ongoing occupation, and to al-Qa’ida’s global insurgency and operations in Iraq, as the international dimension of both of these activities has been well-suited to and heavily supported by the global Internet. Other Sunni insurgent groups in Iraq have also used the Internet to support their efforts to rid Iraq of coalition forces and, in some instances, spread hatred towards Iraqi Shi’ite. The latter illustrates how the Internet has also played a role in Iraq’s sectarian strife.

The US-Iraq Interstate War

Even before the war began in March 2003, the U.S. government launched an e-mail campaign to persuade Iraqi military leaders to not use weapons of mass destruction. According to reports, the Department of Defense sent thousands of e-mail messages in January, promising to protect those who cooperated and their families, but threatening to treat as war criminals those who “took part in the use of these ugly weapons.” In response, the Iraqi government blocked e-mail access to its state-controlled e-mail service in order to keep the messages from circulating.

Hackers took a different approach in their attempts to influence U.S. government officials, posting messages on hacked websites. In September 2002, the cyber intelligence and security firm mi2g reported that the Unix Security Guards (USG), a group of hackers from Egypt, Morocco, Kuwait and Indonesia, alone had recently carried out 155 digital attacks, leaving behind messages such as “Long live Palestine & take your dirty hands off Iraq!” Web attacks escalated after the onset of the war, with estimates of 20,000
defacements, both pro- and anti-war, between mid-March and mid-April 2003. None of these attacks had any impact on policy makers, however.

These two examples illustrate two ways in which the Internet has been used to influence government officials: direct messaging and web attacks. Anti-war activists have also used the Internet to organize and coordinate both online and offline actions, including petition and letter-writing campaigns, street demonstrations and marches, boycotts, and denial-of-service attacks against websites. ANSWER (Act Now to Stop War and End Racism), which was formed in the wake of the September 11, 2001 terrorist attacks, for example, used its website before the invasion for an anti-war referendum and to promote street demonstrations in the United States against the Iraq war. The website has continued to support anti-war actions.

By far the greatest use of the Internet in the Iraq conflict has been for disseminating information such as news, opinion, instructions, decrees, and exhortations. Information is disseminated through websites and forums, blogs, e-mail, and other online media in a variety of formats, to include text, images, audio, and video. Much of the information is intended to influence a target audience and gain their support, but even that which is not has the potential of doing so.

Blogs have played an especially interesting role. During the early “shock and awe” days of the US-Iraq war, when the primary sources of news were US military officers, the Iraq Minister of Information (“Baghdad Bob”), and reporters embedded with US forces, a blogger in Baghdad began writing about what he saw and experienced. His blog, “Where is Raed,” attracted a substantial readership, offering information and perspective that was compelling and not available elsewhere. Since then, hundreds of
Iraqi bloggers have contributed to the inside story from Iraq. US military personnel also began blogging from Iraq, offering some of the best coverage of the Iraq conflict.

The use of the Internet in the telling of the Iraq narrative may have contributed to the pervasive anti-war sentiment. Although any causal link would be difficult to establish, the widespread distribution of images and video clips showing the horrors of war and incidents such as the mistreatment of prisoners at Abu Ghraib, plus countless essays and reports challenging the reasons for invading Iraq and the conduct of the war itself, reflected poorly on the war.

Al-Qa’ida’s Global Insurgency and Operations in Iraq

Al-Qa’ida, and the global social movement inspired by it, has made extensive use of the Internet to distribute information, attract and recruit new members and supporters, finance operations, engage in cyber attacks, and generally communicate amongst themselves.8 Thousands of jihadi websites have supported the movement, carrying audio and video statements by Osama Bin Laden, al-Zawahiri, and other al-Qa’ida leaders; horrific videos of beheadings, suicide explosions, and other acts of terrorism; calls for jihad; and training in such areas as explosives, AK-47s, surface-to-air missiles, poisons, hacking, intelligence, and operations security. In 2007, Al-Qa’ida’s al-Sahab media company alone released 74 videos, about one every three days.9 The high quality products are often posted in multiple languages, including Arabic and English, and in multiple formats such as Windows Media, MPEG4, flash, and a format for mobile devices. By using the Internet, al-Qa’ida has bypassed the mainstream press and taken their messages directly to an international audience. However, their products are also
broadcast by major media such as CNN and al-Jazeera, so al-Qa’ida’s audience is not limited to Internet users.

Before his death, Abu Musab al-Zarqawi, leader of al-Qa’ida’ in Iraq (AQI), used the Internet to post gruesome videos of AQI’s terrorist operations and immortalize their suicide bombers. He started a monthly Internet magazine, offering religious justifications for jihad and advice on how to conduct it, and posted films of his bomb making classes so that his expertise would not be lost. In summer 2005, AQI averaged 9 online postings per day. Two years later, in July 2007, their rate of posting was still high, with 201 for the month (6-7 per day). They used several online media production and distribution entities, including the Al-Fajr Media Center, the Global Islamic Media Front, and the Al-Furqan Media Institute. These entities serve to “brand” jihadist media and post them on the Internet. More recently, AQI postings have dramatically declined, with only 34 in February 2008. This is likely because of the stepped-up efforts against AQI, including the capture or killing of 39 AQI members responsible for producing and disseminating materials on the Internet.

Much of al-Qa’ida’s Internet activity is interactive, taking place in open and closed web forums and groups. Marc Sageman observes that while websites have been instrumental to the al-Qa’ida movement for distributing documents and other materials, it is through the interactive forums that relationships are built, bonding takes place, and beliefs are hardened. He writes, “It is the forums, not the images of the passive websites, which are crucial in the process of radicalization. People change their minds through discussion with friends, not by simply reading impersonal stories.” Sageman believes that the forums are to the current generation of jihadists what the mosques were to the
previous generation. They play a much larger role in al-Qa’ida’s efforts to recruit jihadists than the passive websites, where the visitors are already predisposed to the views that are promulgated. Moreover, it is in conversation that commitments are made, plans are hatched, and actions are put into motion. In today’s networked world, these conversations can as easily be online as in person.

Internet forums have facilitated AQI’s recruitment of foreign jihadists to Iraq. The forum www.nnuu.org, for example, offered instructions to jihadists transiting Syria on their way to Iraq.\(^\text{14}\) Another forum held a live interview with a militant in Iraq, who answered questions about the progress of the conflict in Iraq and how to emigrate and join the fighting.\(^\text{15}\)

Jihadists have also used Internet forums to facilitate cyber attacks. The al-Jinan forum, for example, has been used to plan, organize, and support electronic jihad against websites deemed anti-Islamic.\(^\text{16}\) The objective is to “inflict maximum human, financial and morale damage on the enemy by using the Internet.” Visitors to the forum can download the Electronic Jihad software tool, which automates distributed denial of service (DDoS) attacks against target websites. The forum lists websites attacked and their impact, and gives awards to participants who are the most effective.

Cyber attacks are also used to finance and support al-Qa’ida’s operations. The Moroccan-born British Younes Tsouli, whose online identity was “Irhabi (Terrorist) 007,” hid al-Qa’ida files and communications on websites he penetrated. His 74-page manual “The Encyclopedia of Hacking the Zionist and Crusader Websites” provides hacking instructions and a list of vulnerable websites.\(^\text{17}\) Tsouli also used stolen identities and credit card numbers to pay for web hosting services. To acquire card numbers, he and
his cohorts planted keystroke loggers on their websites and sent out bogus e-mails with links to websites requesting financial information. His websites featured materials from Zarqawi and AQI.18

**Countering al-Qa’ida**

Much has been written about how to counter al-Qa’ida and its global social movement. Especially recommend are Marc Sageman’s book19 and reports by J. Rami Roz,20 Robert Martinage,21 and Frank Ciluffo et al.22 Here we discuss four strategies that are explicitly directed at al-Qa’ida’s Internet presence: intelligence collection, denial, subversion, and engagement.

The first strategy, intelligence collection, is to monitor al-Qa’ida’s Internet forums and message exchanges in order to develop actionable intelligence regarding al-Qa’ida members and their social networks; safe houses and other facilities where members gather and weapons are produced; proposals and plans for terrorist acts; financial sources and transactions; and other relevant information. Information gleaned from such surveillance can be used to facilitate arrests, confiscate weapons, and thwart plots. Law enforcement and intelligence agencies already engage in such monitoring, and it has been valuable in the fight against al-Qa’ida. As noted earlier, the effect of “capture or kill” operations against AQI have had the added benefit of curtailing their media campaign.

The second strategy, denial, is more controversial. The goal is to take actions that deny al-Qa’ida access to the Internet, for example, by shutting down their e-mail and IM accounts, and their websites and forums. The premise is that by getting al-Qa’ida off the net, they will be unable to post materials and engage with potential recruits. Further,
communications among jihadists will be severely hampered, making it more difficult for them to plan and organize actions. While these results can be beneficial, the approach also has problems and limitations. One is that it is easy to establish new Internet accounts and reinstate websites and forums in new locations, so removal at best impairs al-Qa’ida’s efficiency. Moreover, because jihadists can access the Internet from an Internet café or any other place with Internet access, they cannot be denied access by targeting a particular access point, say at a known safe house or particular cyber café.

In addition to removing accounts and websites, denial can be approached by censoring certain Internet traffic. For example, AQI might be denied access to the Internet by monitoring all Internet communications coming into and out of Iraq, blocking anything that appeared to relate to al-Qa’ida. However, it would be extremely difficult to develop filters that would distinguish al-Qa’ida traffic from other traffic, especially given their practice of using code words to hide the meaning of messages. In addition, the jihadists have their own encryption tool, Mujahedeen Secrets, for concealing the content of files and messages. The software is based on strong, well-vetted ciphers, including the Advanced Encryption Standard (AES) and RSA. On top of that, there are software tools for bypassing Internet filters. The net effect is that filtering would not be fullproof, yet would almost certainly suppress legitimate traffic, thereby violating human rights.

Another problem with denial is that much of the content on jihadi websites is permissible under principles of free speech. Hence, removal is impossible without compromising human rights, especially if materials are posted for information purposes on non-jihadi sites. Denial also has adverse effects on intelligence collection, potentially taking away valuable sources of information as jihadists move further underground on the
Internet or conduct their operations entirely off-line. Finally, denial requires international cooperation to be fully successful, as jihadi accounts and websites can be hosted all over the world. Such cooperation can be difficult to achieve. Still, making al-Qa’ida less efficient and on the run has merit, so denial may be appropriate when there is a clear violation of laws and potential gains. Indeed, it is already practiced by ISP’s to remove websites that directly advocate violence or provide support to known terrorist organizations.

The third strategy, subversion, is also controversial. It involves infiltrating al-Qa’ida forums, disrupting their operations, and using deception to subvert al-Qa’ida objectives, for example, by injecting misinformation into a forum discussion in order to erode trust in an al-Qa’ida leader or undermine a planned terrorist operation. This strategy is risky, as operations can have unintended consequences and backfire. Also, if not coordinated with intelligence operations, they can undermine collection efforts and lead to false conclusions. However, the strategy should not be dismissed outright, as deceptive techniques can be effective.

The fourth strategy, engagement, takes a more positive approach. The idea is to converse with jihadists and potential recruits, challenging basic premises and beliefs through dialog and writings. The goal is to draw people out of the movement and deter potential recruits from joining. If indeed it is through conversations in web forums that potential recruits are radicalized and become committed to the jihad, then alternative conversations may be employed to lead them in the opposite direction. Saudi Arabia’s online Al-Sakinah (“Tranquility”) campaign illustrates. Muslim scholars and sheikhs with expertise on Islam, aided by experts in sociology and psychology, enter extremist web
forums and engage with participants, encouraging them to renounce their extremist ideas. According to reports, the campaign has been successful. About 700 individuals recanted their beliefs, including high-ranking members of al-Qa’ida.23

For engagement to succeed, speakers must be able to develop rapport and trust with their target populations. Ideally, they should come from the same ethnicity, religion, and culture, as in the Saudi Tranquility campaign. In general, people are more influenced by those that are like them than those that are not.

Of these four strategies, the first three require that al-Qa’ida operatives and their Internet sites be accurately identified. Otherwise, innocent persons could be swept up in counterterrorist operations. This could be particularly harmful with strategies based on denial and subversion, adding to the problems already associated with these approaches.

Although all four strategies have value, we recommend emphasizing intelligence collection, followed by engagement. Denial and subversion may be used, but only under conditions where there are clear benefits and minor risks. A strategy that focuses primarily on getting jihadists off the Internet is likely to severely undermine intelligence collection against al-Qa’ida, while compromising the civil liberties of innocent persons caught in the sweep. Moreover, it is not likely to work.

Endnotes

5 “Digital Conflict Over Iraq Has Begum,” Mi2g, September 10, 2002.
This information is based on the author’s own observations of ANSWER’s website at http://www.internationalanswer.org/ since early 2003.

Much has been written on this. See for example Gabriel Weimann, *Terror on the Internet*, United States Institute of Peace Press, Washington DC, 2006.


Marc Sageman, *Leaderless Jihad*.


