

Cell Phone Use by Insurgents in Iraq

By
Tiffany Strother

14 May 2007



Urban Warfare Analysis Center

Shawnee, OK
(405) 273-3035

Cell Phone Use by Insurgents in Iraq

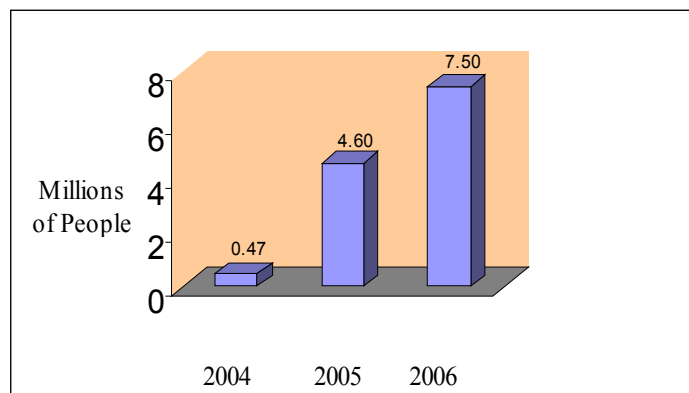
SUMMARY

Since the official availability of commercial cell phones in Iraq in 2004, Iraqi insurgents have developed numerous applications for them. The convenience, mobility, low cost, accessibility of information, and technological capacity of mobile phones has drastically enhanced the connectivity and collaboration of insurgents. This, in turn, has provided insurgents in Iraq new opportunities to circumvent counter-insurgency (COIN) efforts. It also has fostered unprecedented situational awareness in combat. As cell phone technology evolves, insurgents will continue to use cell phones to increase the efficiency and impact of their operations.

BACKGROUND

Cellular service first became available in Iraq in January 2004 after the fall of Saddam's Baathist regime.¹ At first, cell phone service cost as much as \$1,000 per month.² As the demand for service increased, prices dropped precipitously. Currently, cell phone service costs as little as \$40 a month.³ At present, 89 percent of Iraqis own cell phones, compared to only 6 percent in 2004.⁴

Mobile Phone Subscribers in Iraq



Sources: CIA, World Market Research, and U.S. Commerce Department

Modern insurgents in Iraq now use cell phones to coordinate the activities of their many decentralized networks.⁵ Unlike previous insurgencies with hierarchical organizations designed to maintain command and control, insurgents in Iraq--such as Tadhim al-Qa'ida fi Bilad al-Rafidayn (al Qaeda's organization in Mesopotamia) and Ansar al-Sunna (Partisans of the Sunna Army)--use cell phones widely to exchange information

and coordinate activities.⁶ This model of multiple small hubs in constant communication with each other is one of the main reasons insurgents in Iraq have adapted faster than insurgencies elsewhere.

The advent of disposable mobile phones also has increased their appeal to insurgents in Iraq. In particular, the process of attaining a pre-paid or disposable mobile phone is less cumbersome than that of a conventional cell phone. In most cases, acquiring a regular cell phone consists of registering the phone, providing valid identification documentation for purchase verification, and other measures that can be traced. In contrast, pre-paid phones often do not require registration or even a name when purchasing, therefore providing little evidence for investigating authorities to track. If a call (originating or received) from a disposable phone is selected for monitoring, authorities have few means to identify who is talking.⁷

- The low cost of disposable mobile phones adds to their appeal. They usually cost several hundred dollars cheaper than a conventional cell phone in Iraq, which can be as high as \$800.⁸ As a result, they can be used for one day and thrown out, with a new phone (and a different number) activated the next day.⁹

VARIOUS USES

Insurgents in Iraq have employed cell phones for a wide range of uses. Detonating IEDs is the most deadly and widely known use of cell phones in Iraq. Nonetheless, Iraqi insurgents have adapted and employed mobile phones in other endeavors not as deadly but significantly damaging to COIN efforts. This is most evident in the area of communications. Insurgents have constructed “mobile command and control centers” enabling them to exchange information quickly.¹⁰ The most common uses of cell phones by insurgents in Iraq are discussed below.

IED Triggers

The use of cell phones as triggers for IEDs has been highly publicized and remains by far the most deadly use of cell phones by Iraqi insurgents. As of May 2007, U.S. deaths by IEDs numbered 1,359 -- almost half of the 3,389 U.S. service members who have lost their lives since the invasion of Iraq.¹¹

There are two main methods for constructing an IED with a cell phone trigger. The first and most widely used is the “call in” technique. The explosive material is wired to a mobile phone; a second phone is then used to call the number of the wired phone. The small charge generated from the call ignites the bomb.¹² This technique provides the most accuracy as a spotter can watch the site and control when the IED is detonated, providing maximum effectiveness.



Picture of cell phone used to trigger an IED.
Source: LiveJournal.com

- In one example of this method, U.S. troops seized a video that shows insurgents in a car that passed an Army convoy going in the opposite direction. When the convoy reached a certain point, the men in the video can be seen using a cell phone to detonate a hidden IED.¹³

The second technique for detonating IEDs works similar to the first, except that the internal alarm on the phone is set as a timer. When the timer goes off, the alarm detonates the explosive.¹⁴ This method does not allow for the flexibility and precision of the first technique and requires more extensive knowledge and planning of the target to be successful.

Sitreps

Mobile phones are often used as a vehicle to coordinate and disseminate situation reports (sitreps) containing information relative to tactics, techniques, and procedures. Insurgents can communicate their positions to each other, monitor and report on troop movement, and update the status of operations in real time.

- For example, as reported in Baghdad in November of 2005, an insurgent was caught lurking on a rooftop watching an IED attack while talking on his cell phone.¹⁵ In instances such as this, the spotter may be relaying the results of the attack. In other cases, the spotter looks to detonate additional bombs.

UNCLASSIFIED

The ability of a fighting force to receive accurate and timely information of the battle environment is a necessary and difficult task. It often defines the lines of success for an operation. Insurgent use of cellular phones in Iraq provides them with situational awareness approaching that of well trained armies, greatly leveling the playing field against technologically advanced adversaries.

Text messaging

Another method used to transmit information is short message service, otherwise known as text messaging. It is widely favored by insurgents because it is difficult to track and even more challenging to disrupt.

One technique in particular involves texting one part of a message to a cell phone, hanging up, and calling a different phone to send the other part.¹⁶ This technique requires the insurgent on the receiving end to possess more than one cell phone. The main benefit is that the message is virtually untraceable.

The smaller bandwidth used to send a text message also makes the application more reliable than actually placing a call. Thus, the enemy may conduct operational security (OPSEC) at a fraction of the cost and training required for conventional methods.

- During the 9/11 attacks, networks and telephone lines were jammed from the massive volume of calls being made, but text messages were unaffected.¹⁷
- Khalid Shaikh Mohammed, the driving force behind the 9/11 attacks, consistently used cell phones to communicate important information. Several months after the attacks, he was seen handling four to five phones at once sending and receiving text messages.¹⁸

Multimedia Messaging Service

The ability to send a picture or video from one mobile phone to another (or to the Internet) is another tool Iraqi insurgents have manipulated for their own purposes. Multimedia messaging is an enhanced transmission service that enables graphics, video clips, and sound files to be transmitted via cell phone.

- For example, a camera phone was used to film the hanging of Saddam Hussein. The clip, which was subsequently released via the Internet within hours, garnered world wide attention and caused a sharp reaction among the Sunni community in Iraq. Thousands of Sunnis protested in the streets of Anbar province, while a main thoroughfare in Fallujah was later named the Street of the Martyr Saddam Hussein, inviting anti-Shiite animosity.¹⁹

Insurgents in Iraq have also used camera phones to gather visual information against U.S. and coalition targets. Pictures of unit patches, rank, and even bumper numbers of military vehicles have all been discovered on the cell phones of captured insurgents.²⁰ Moreover,

UNCLASSIFIED

the pictures taken are not random. The information is used to distinguish and track targets and high ranking officials as well as assist in the planning and execution of attacks against those targets.

- One army commander, who has served several tours in Iraq dating from the Gulf war to the present war, recalls numerous pictures that were stored in cell phones of Iraqi insurgents. He states that insurgents would discover the identity of commanders of targeted units, snap a picture of that official, and disseminate the photo among their ranks with a bounty attached.²¹
- There are even instances of insurgents who managed to infiltrate military facilities in Iraq as working civilians, or utilize civilians who are sympathetic to their cause, to conduct reconnaissance missions.²² The insurgents use their camera phones to discreetly take pictures of the daily operations conducted on the post, including the inside and outside of buildings and the rotations of units performing guard duty, to create a detailed map for attack purposes.²³

Propaganda

Advancements in cell phone technology have provided a simplified, more flexible avenue for insurgents to drastically enhance their ability to disseminate their own interpretation of events. Gathering support--and by extension funding, recruits, and supplies--are critical for developing and maintaining an insurgency. The assiduous application of methods designed to incite the populace or exaggerate the insurgency's effectiveness radically help to further their cause.

- For example, footage of U.S. soldiers being shot or blown up has been set to popular music, providing two major impressions. First, the only footage displayed is of soldiers dying; spawning the belief that the U.S. and their allies are losing the war. Second, the music and editing appeal to cultural norms and fads to inspire future recruits, especially young people.²⁴

Abetting Crime

Criminal activity conducted by insurgents--and greatly enhanced by the use of cell phones--has proven to be a major source of funding for radical elements. For example, kidnappings in Iraq have greatly advanced through the use of cell phones, with the average ransom for a kidnapped victim now reaching around \$25,000.²⁵

- One occurrence of kidnapping, symbolic of the many, involved an Iraqi civilian in which the ransom demand was delivered to his brother's cell phone. The brother paid the \$15,000 ransom for the release of his brother. After receipt of the money, he was directed to the place where he could find his brother, who had already been killed.²⁶

UNCLASSIFIED

- The rise of crime facilitated, in part, by cell phones has some Iraqi civilians preferring the harsh oppression of Hussein's rule, when cell phones were virtually nonexistent and landlines heavily monitored.²⁷

COUNTERMEASURES

The counter measures employed against cell phones used by Iraqi insurgents are rudimentary, sometimes hindering coalition troops more than they disrupt insurgent activity. Some of the counter measures that have been applied, including their effectiveness and vulnerabilities, are listed below.

Jamming

Electronic jammers in Iraq are operated specifically to counteract the detonation of IEDs by remote devices, such as cell phones, garage door openers, and hand held radios. Jamming is the intentional generation of interfering signals by powerful transmitters intended to prevent clear reception of broadcast signals.²⁸

The military's considerable efforts to date on jamming techniques have produced mixed results. In 2006, the Pentagon spent \$1.4 billion on jamming efforts, almost half of the \$3.5 billion used to combat the IED problem.²⁹ In that same year, the United States military bought 3,800 electronic jammers for \$79,000 each from General Dynamics and more than 4,000 Warlock jammers from EDO Corp at \$200,000 per jammer.³⁰

- The Warlock jammer, previously tested in 2005, has gone through numerous remodifications and is currently available in two main versions in Iraq -- the compact Humvee mounted combo and the man-portable Blue model attached to a soldier's vest.³¹ The Warlock, and other systems like it, are classified. Therefore, specific information about its capabilities is not available in open source documents.
- Jammers are also mounted on aircraft, such as the Marine Corps EA-6B Prowler's communications jammer, which intercepts radio signals and prevents them from reaching their destination.³² The Air Force Compass Call airborne jammer has the same capability as the Prowler, but on a larger scale.³³

Jamming efforts have had some success. For example, a U.S. lieutenant who served in a unit in Iraq that utilized the Warlock jammer recalls that "IEDs would explode just as they passed outside the range of the unit's Warlocks, perhaps indicating that insurgents were trying to detonate the devices as patrols passed and that Warlocks temporarily blocked the signals."³⁴

The use of jammers in Iraq has caused unfortunate side effects, however. As Iraqi insurgents became more inventive with their triggering techniques, more powerful

UNCLASSIFIED

jammers were needed to combat the adaptations. As a result, jammers have become so powerful that they sometimes disrupt friendly communications in addition to their intended purpose.

- For example, in March 2005 a patrol from the 25th Infantry Division near the northern city of Mosul had its communications briefly wiped out when a Compass Call passed overhead. All radio signals in the area were jammed.³⁵
- The operation of military radios (UHF, VHF, HF man packs, tactical satellite systems, etc.) can also negate the effectiveness of jammers. As a result, in January 2007 the Naval Sea Systems Command issued a request for private industry to develop an interference mitigation system that would enable simultaneous operation of IED jammers and tactical communications within the same location or vehicle.³⁶

Jamming techniques face the same challenges as other COIN strategies--constant adaptation by the enemy. Jamming only remains effective for the amount of time it takes insurgents to develop new methods of detonating IEDs. Pressure plates and passive infrared beams are now used as triggering devices, which render jamming efforts useless.

Monitoring Cell Phone Activity

Monitoring cell phone activity among insurgents can illuminate the goals and activities of a modern insurgency. In particular, the networks created by Iraqi insurgents are vulnerable to exploitation because of their decentralized nature. The use of cell phones by the many participants in those networks increases their risk of exposure to COIN efforts. For example, analysts can monitor links between insurgents to establish connections from one insurgent to another, eventually compromising an entire network and leading to arrests.³⁷ The impact of information gleaned from just one arrest can ripple throughout the entire organization.³⁸

- One illustration of this occurrence was the capture of Abu Zubaydah. There are conflicting accounts as to the value of Zubaydah in connection with al Qaeda, but his capture led to several actionable pieces of intelligence. A myriad of valuable "eavesdropping" sources were discovered, including e-mail addresses, cell phone numbers, and personal phone directories.³⁹ Monitoring these sources led to the capture of other al Qaeda operatives, most importantly Khalid Shaikh Mohammed, plus the exposure of future operations.
- The former leader of al Qaeda in Iraq, al Zarqawi, also was tracked and killed through his use of a cell phone in June 2006.⁴⁰

There are several systems in use today that are designed to monitor communications among insurgents in Iraq. Specific details concerning the exact nature and function of these systems are classified. However, the Patriot Act--ratified shortly after 9/11 and which allows greater authority in tracking and intercepting communications--has been

UNCLASSIFIED

attributed to the capture of several insurgents (Mohammed in particular). This suggests these systems have been successful at aiding COIN forces and other governing authorities.⁴¹

- Echelon is an example of one such monitoring device. It is a global eavesdropping system utilized by the National Security Agency (NSA) to collect foreign intelligence.⁴² If a foreign intelligence source calls the United States or if a domestic source contacts a foreign national who the NSA is already monitoring, the NSA monitors that communication via Echelon or other means.⁴³

OUTLOOK

The use of mobile phones by insurgents in Iraq is likely to escalate. Moreover, a new generation of cellphone technology is launched approximately every 12-18 months, and Iraqi insurgents will use it to adapt to future fighting conditions.⁴⁴ Whether as a physical weapon--triggering IEDs--or less direct methods involving communications, this powerful tool will continue to amplify the effect of insurgent activity in Iraq.

IED Triggers. Although other methods of triggering IEDs have and will continue to be developed and utilized, cell phones will continue to play a significant role. Other triggering devices, such as pressure sensors and infrared lasers, are costlier than cell phone use and not as readily available. The acquisition of these other devices may also raise scrutiny among COIN and police forces. Moreover, the training and support activities required for their use are costly and burdensome compared to the simplicity of cell phones.

- According to an article released by the Marine Corp Times in September 2006, British military intelligence forces assess that there are enough stocks of illegal explosives in Iraq to continue the same levels of IED attacks for 274 years without resupply.⁴⁵ Such unlimited access to bomb making material and the ease of cell phone use strongly indicate the continued use of cell phones as triggering devices.

Text Messages. Text messaging has many possibilities and will most likely continue to be utilized as a quick and efficient means of communication among insurgents. In addition, when used in conjunction with computers, the impact of this activity increases exponentially in scope.

- Mass emails sent to cell phones containing actionable information--target specifications or times and locations of attacks--will continue to present challenges for COIN forces due to the difficulty involved in tracking text messages.

UNCLASSIFIED

If applied as a defensive measure, however, text messages could aid COIN efforts. More than three quarters of the Iraqi population possess cell phones and text messaging could be an effective means for U.S. officials to communicate with the Iraqi people.

- In New South Wales, an early warning message system has been created that allows emergency services to send alerts to cell phones across all networks within a possible terrorist target zone.⁴⁶
- British Intelligence has created a link on their website where civilians can sign up to receive email alerts directed to a cell phone whenever there are changes to the nations threat level.⁴⁷

Multimedia Message Service. Insurgents in Iraq already use mobile phones for reconnaissance purposes. As cell phone technology expands they are likely to continue to manipulate cell phone innovations to add visual and other information to text messages.

- Steganographic MMS messages could increasingly be used to send vital information--maps and pictures of targeted installations--in an effort to coordinate and execute attacks. Steganographic messages were used to plan the 9/11 attacks and could be used more frequently in the future.⁴⁸
- Insurgents in India routinely send information steganographically via cell phones. In February 2007, officials in India describe intercepting messages containing information on insurgent activities, money laundering, and even an attack on Parliament.⁴⁹

MMS could also be used to the advantage of COIN and policing forces in Iraq. For example, a picture or text message concerning information of suspected terrorists could be disseminated to soldiers operating check points via mobile phones designated specifically for that purpose.

- In addition, civilians could send pictures or video clips of insurgents “caught in the act” to authorities. Once screened, information deemed legitimate could be redistributed to soldiers at check points or surrounding areas of operation.

Propaganda. Enhanced ease of communication via cell phones will allow insurgents greater opportunities to disseminate their ideology and explain the “benefits” of their actions, likely leading to more recruits. Indeed, one of the most important advantages of mobile phones for insurgents in Iraq is increased unity of purpose. Cell phones are one of many tools that have allowed insurgents to bond under a common goal.

Nonetheless, increased communication could have negative consequences for the insurgents as well, especially as the fighting drags on. Overly acerbic propaganda is one area where insurgents in Iraq could be the instrument of their own demise. As Iraqi insurgents continue to fervently spread their ideals and opinions concerning Islamic

UNCLASSIFIED

beliefs, the possibility for dissent rises, potentially fracturing the ranks and weakening the insurgency. Any internal splits will create vulnerabilities for COIN forces to exploit.

- For example, an Internet posting by the Islamic Army in Iraq last month sharpened differences among radical Sunni groups.⁵⁰ The posting strongly opposed the killing of Sunnis, which distanced the group from al Qaeda and others.

UNCLASSIFIED

ENDNOTES

- ¹ Aws al-Timimi, "Cell Phones Bring More Sadness to Iraq," The Augusta Chronicle (Georgia), 30 Sept. 2006: pA05.
- ² al-Timimi, pA05.
- ³ al-Timimi, pA05.
- ⁴ Good Morning America, ABC, New York, NY, 19 Mar. 2007.
- ⁵ Martin J. Muckian, "Structural Vulnerabilities of Networked Insurgencies: Adapting to the New Adversary," Parameters, Winter 2006-07: p15.
- ⁶ Muckian, p16.
- ⁷ Investigative report conducted by Brian Ross, "Terror Cells," Information provided by the Federal Bureau of Investigation and interviews from former FBI agent Jack Cloonan, Good Morning America, ABC, New York, NY, 13 Jan. 2006.
- ⁸ Damien Cave, "Must Haves: Cell Phones Top Iraqi Cool List," The New York Times, 8 Aug. 2006, 23 Jan. 2007, <http://www.nytimes.com>.
- ⁹ "Terror Cells", 13 Jan. 2006.
- ¹⁰ Rowan Scarborough, "Cell Phone Technology: An Explosive Tool for Insurgents," The Washington Times, 7 Mar. 2005: pA01.
- ¹¹ Michael White, "Iraq Coalition Casualty Count," 9 May 2007, <http://icasualties.org/oif/IED.aspx> and <http://icasualties.org/oif/default.aspx>.
- ¹² Mike Angell, "Handsets' Deadly Use: Detonators; A Tool for Terrorist Bombers; Jamming Devices can Stop Explosions; Carriers Urged to Help Diffuse the Problem," Investor's Business Daily, 29 Aug. 2005: pA06.

UNCLASSIFIED

¹³ Scarborough, pA01.

¹⁴ Angell, pA06.

¹⁵ “Joint Iraqi Ops Keep Terrorists on the Defensive,” Department of Defense News, 20 Nov. 2005.

¹⁶ Scarborough, pA01.

¹⁷ PR Newswire, “Colleges and Universities Can Increase Public Safety Overnight by 90% with New e2Campus 2.0 Mass Notification System; Its Capabilities Include Using SMS Text Messages to Help Schools Instantly Communicate with Entire Campus or Specific Groups Such as a Dorm, Branch Campus or Facilities Crew,” PR Newswire Associates LLC (New York), 18 April 2006, 17 Mar. 2007, <http://prnewswire.com>.

¹⁸ CNN Newsroom, CNN, International edition, 24 Sept. 2006.

¹⁹ Scott Johnson, Michael Hastings, and Benjamin Sutherland, “We’re Losing the Infowar; Insurgents Using Simple Cell Phone Cameras, Laptop Editing Programs and the Web are Beating the United States in the Fierce Battle for Iraqi Public Opinion,” Newsweek, 15 Jan. 2007: p30.

²⁰ Major John Harkins, personal interview, 3 May 2007.

²¹ Harkins, interview.

²² Staff Sergeant Gerald A. Simpson, personal interview, 11 Apr. 2007. In many situations, insurgents who manage to get inside a military installation to perform visual operations also memorize the exact amount of steps from entry point to a high value target--a dining facility or soldier barracks--and use that information to coordinate mortar attacks with greater accuracy. This tactic has proven to be highly accurate.

²³ Harkins, interview.

UNCLASSIFIED

- ²⁴ Johnson, Hastings, and Sutherland, p30.
- ²⁵ Muckian, p22.
- ²⁶ al-Timimi, pA05.
- ²⁷ al-Timimi, pA05.
- ²⁸ Wikipedia, 17 Mar. 2007, <http://wikipedia.org>.
- ²⁹ Tom Vanden Brook, "Jammers Foil IEDs, but also Troops' Radios; Goal: Interference-Proof Communications Systems," USA Today (Washington), 23 Jan. 2007: p6A.
- ³⁰ Robert Bryce, "Surge of Danger for U.S. Troops," Salon News, 22 Jan. 2007, 19 Mar. 2007, <http://www.salon.com/news/features/2007/01/22/ieds/index.html>.
- ³¹ David Axe, "Bomb Sweep: Soldiers, Marines Team Up in 'Trailblazer' Patrols; Battlefield Technology," National Defense (Al Taqaddum Air Base), 1 Apr. 2006: p26.
- ³² Axe, p26.
- ³³ Axe, p26.
- ³⁴ Axe, p26.
- ³⁵ Axe, p26.
- ³⁶ Bob Brewin, "Counter-IED Systems Jam Tactical Comms in Iraq," FCW Media Group, 5 Jan. 2007, 19 Mar. 2007, <http://fcw.com/article97264-01-05-07-Web>.
- ³⁷ Stefan Leader and Charles Russo, "Ripples in the Pond" The Journal of Counterterrorism and Homeland Security International, Summer 2005: Vol. 11.
- ³⁸ Leader and Russo.
- ³⁹ Jack O'Neill, "Connecting the Dots," The Washington Times, 26 Dec. 2005: pA16. Jack O'Neill worked in the White House under President Carter as a

UNCLASSIFIED

telecommunications policy analyst. He is the author of "Echelon, Somebody's Listening" (Washington Times).

⁴⁰ Day to Day, "Zarqawi Strike an Operation Years in the Making," NPR, Washington D.C., 8 Jun. 2006.

⁴¹ Wikipedia, 10 May 2007, <http://wikipedia.org>.

⁴² O'Neill, pA16. Other eavesdropping systems mentioned in Jack O'Neill's novel include: Carnivore, which intercepts internet traffic and Magic Lantern, which decodes encryption.

⁴³ O'Neill, pA16.

⁴⁴ Greg Grant, "No 'Silver Bullet' to Counter IEDs; As Attacks Increase, Researchers Focus on Intelligence as well as Technology," Marine Corp Times, 18 Sept. 2006: p12.

⁴⁵ Grant, p13.

⁴⁶ "Across Asia Australia," 27 Feb. 2007, 11 Apr. 2007, <http://www.chinadaily.com.cn/>.

⁴⁷ Jeffrey Stinson, "Britons Can Sign Up For E-mail Terror Alerts; Country's MI5 Agency Emerges From Secrecy," USA Today (London), 10 Jan. 2007: p8A.

⁴⁸ "Software to Combat Hi-Tech Crimes," Indo-Asian News Service, 18 May 2005.

⁴⁹ "Terrorists Start Reading Between the Lines," The Statesman (India), 1 Feb. 2007.

⁵⁰ Steven R. Hurst, "Suicide Truck Bomber Explodes Chlorine Bomb, Kills 27," Associated Press Worldstream (Baghdad), 6 Apr. 2007. In part, the posting stated, "al

UNCLASSIFIED

Qaeda was killing fighters of the Islamic army and other militant Sunni groups if they did not pledge loyalty to al Qaeda.”

UNCLASSIFIED