

# Terrorism and Bluetooth

Steve Gold, freelance journalist

**The recent confirmation of the veteran second-in-command of al-Qaeda, Ayman al-Zawahiri, as the new leader of the infamous terrorist group – following the US-led ‘removal’ of Osama bin Laden in his Pakistan headquarters in early May – will not have gone down well with the US administration. The reason is that al-Zawahiri is even more hostile towards the West than bin Laden, as has recently been confirmed by his press statements committing al-Qaeda to a holy war – a Jihad – against the US and Israel. To pursue this campaign, the organisation needs to spread its message. And while the Western media likes to portray al-Qaeda as a low-tech, unstructured organisation, the reality is that the global group makes significant use of digital technology to promulgate its subversive message and recruit new members.**

Al-Qaeda has a digital research and development arm known as the Fariq Jawwal Al-Ansar (FJA) which, despite the ubiquitous nature of the Internet, has eschewed the web and email as its main means of communication in favour of Bluetooth technology. The reason for this is that, unlike the Internet, which is accessible to almost anyone with an IP connection, Bluetooth is a short-range Personal Area Network (PAN) with a maximum transmission range of 100m (using a Class 1 100mW transmitter). Al-Qaeda regards the technology as a perfect pocket-to-pocket broadcast mechanism that is almost undetectable by Western intelligence agents.

***“Where digital jihadists once used the multimedia features of the web to communicate and proselytise, there is strong evidence that they are now using Bluetooth PAN technology to distribute digital magazines on a pocket-to-pocket basis”***

According to Nigel Stanley, security practice leader with Bloor Research, websites such as Jihadica.com show the reliance that al-Qaeda now places on mobile phone technology to broadcast its jihadist messages of hate to existing members and potential new recruits. Where digital jihadists once used the multimedia features of the web to communicate and proselytise, there is strong evidence that

they are now using Bluetooth PAN technology to distribute digital magazines on a pocket-to-pocket basis.

## Always on

Nico Prucha, a Vienna-based researcher who is undertaking doctoral research in the jihadist use of digital technology to recruit new members, reports that the FJA has been using Bluetooth as a narrowcasting medium for at least the past two years. Unlike in the West, where smartphone users typically toggle the Bluetooth feature of their mobiles as discoverable when they are attempting to pair their handset with another Bluetooth device, most young people in Arab/Middle Eastern nations – such as Afghanistan, Iran and Pakistan – leave their Bluetooth feature as discoverable all the time. The reason for this, says Prucha, is the strict moral code of these countries prohibits direct interaction between members of the opposite sex, so the teenagers use technology such as Bluetooth to make new friends and do what youngsters have done since time immemorial.

This is where the FWA has developed and refined a Bluetooth narrowcasting strategy to transmit digital magazines from mobile Class 1 (100mW) transceivers to any and all Bluetooth mobiles in the area. Even though most smartphones operate as Class 2 (2.5mW) or Class 3 (1.0mW) Bluetooth devices, effective over ranges

of 5-10m, they can still receive a Class 1 Bluetooth signal at range of up to 100m.

According to Stanley, the digital magazines that are transmitted by al-Qaeda – and which are retransmitted on a pocket-to-pocket basis between like-minded individuals – are very slick affairs, containing video footage of the plane-bombing of the New York Twin Towers a decade ago, all the way through to the ritual beheadings of hostages captured by the jihadists.

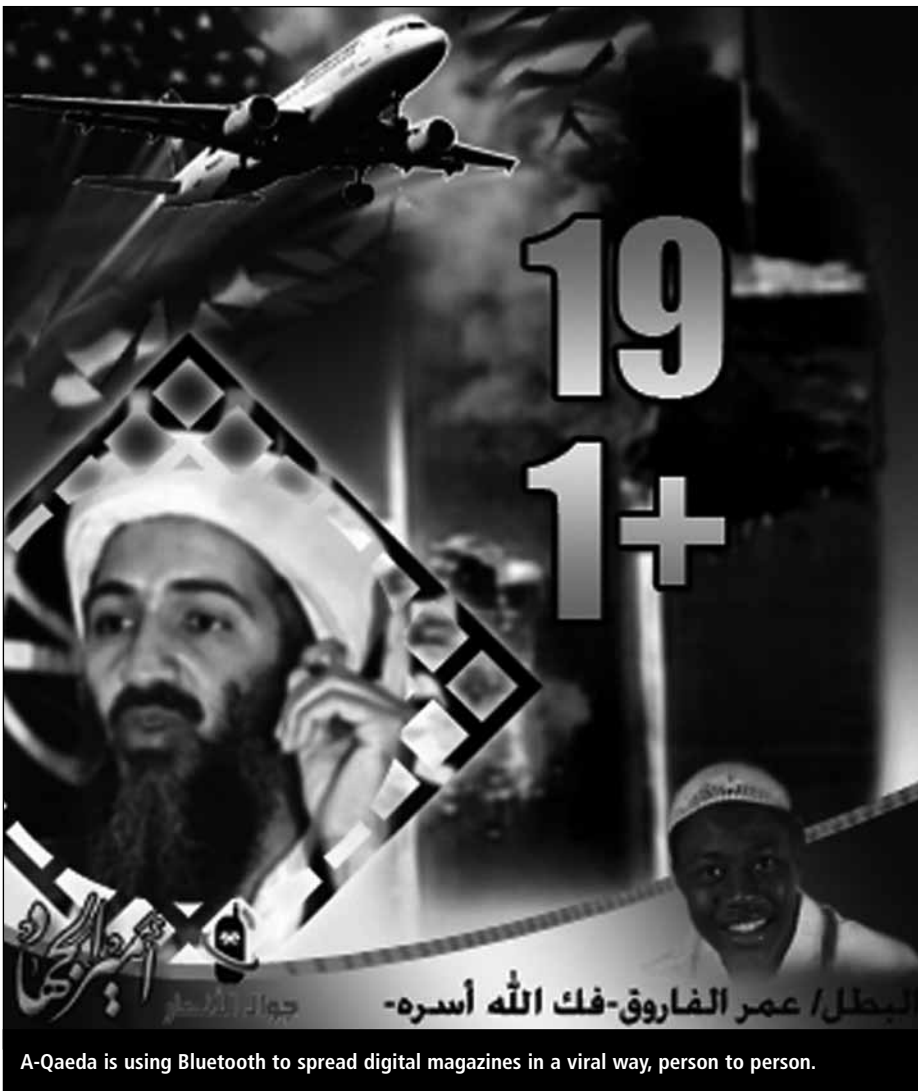
Prucha, who works with the Austrian Institute for International Affairs, says that al-Qaeda’s FJA detachment has been refining its Bluetooth narrowcasting techniques for some time, and uses the technology as a channel for viral propaganda. In fact, Prucha claims that without digital technologies such as the Internet and smartphones, al-Qaeda as a terrorist organisation would have faded away long before today. In pre-Internet times, he says, al-Qaeda would have used videotape magazines to propagate its messages and, if you copy a tape 10 times, the quality is extremely poor.



Steve Gold



Nigel Stanley, Bloor Research.



A-Qaeda is using Bluetooth to spread digital magazines in a viral way, person to person.

With digital media, he says, no matter how many times you copy the media, the content remains the same quality.

## Understanding Bluetooth technology

Before we discuss how Western agencies can tackle the problem of Bluetooth pocket-to-pocket transmissions, it's helpful to understand how the technology works. The Bluetooth specification was actually developed as a replacement for RS-232 cabling back in 1994 by two Ericsson researchers, Jaap Haartsen and Sven Mattisson. Based on low-power, spread-spectrum technology, the Bluetooth Special Interest Group (SIG) started operations in 1998 and, within a few years, most mobile phones started featuring the technology as a low-power precursor – and now alternative – to battery-hungry wifi transmissions. Because Bluetooth operates on a spread-spectrum basis in the short wavelength

radio spectrum known as the Industrial, Scientific and Medical (ISM) band (2400-2480MHz), it can reach much greater distances than analogue discrete channel transmissions of the same power.

In its earliest iterations, Gaussian Frequency-Shift Keying (GFSK) modulation was the only modulation scheme available. But by the time the Bluetooth 2.0 standard was ratified in 2004, other faster modulations – 4-DQPSK and 8DPSK – started being supported. Like TCP/IP, Bluetooth is a packet-based protocol with a master-slave structure. One master can communicate with up to seven slaves in a piconet, with all devices sharing the master's clock. In this *ad hoc* computer network, devices can switch roles, by agreement, with the slave then becoming the master.

It's also worth noting that the Bluetooth core specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simulta-

neously play the master role in one piconet and the slave role in another. This means that a Class 1 Bluetooth transceiver can create a mesh-like net of several piconets in its vicinity, which is ideal for digital magazine transmission sharing, especially when each Bluetooth mobile automatically supports mesh-like behaviour.

## Subverting al-Qaeda transmissions

Because the FJA Bluetooth transmissions take place in Western-hostile countries such as Afghanistan, Iran and Iraq – as well as marginally hostile countries such as Pakistan – the digital magazines are discussed and transmitted between like-minded individuals on a viral distribution basis. Thus, while the initial narrowcasts take place in city areas from Class 1 al-Qaeda Bluetooth transceivers, once the magazine has been seeded to sufficient supporters, a viral propagation effect takes over, with smartphone users distributing the e-magazines between themselves on a semi-automatic basis.

There is evidence to suggest that many teenagers, while not supporting the jihadist principles of al-Qaeda, exchange the e-magazines out of a natural curiosity and a fascination with videos of beheadings that would otherwise be banned on the Internet and regular TV transmissions. This fascination aspect is central to the psychology of the FJA's digital media strategy and, while a large percentage of teenagers will simply view the digital magazines and move on with their lives, there will inevitably be small numbers of recipients who, for various reasons, are susceptible to the teachings of al-Qaeda.

Prucha observes that the main motivation of the FJA is to promote and spread jihadist materials by any and all means, with the express aim of propagating its message of hate, and recruiting new members to the cause. He adds that the FJA, "considers itself as yet another platform to disseminate, proselytise and hence protect the 'true version' of religion."

## Technical countermeasures

Like all forms of propaganda, it is difficult to counter these digital magazines

using conventional arguments, so the difficult question facing Western allies is how to subvert these Bluetooth narrowcasts. Unconfirmed reports suggest that Western soldiers have been deploying Bluetooth signal jammers that block the control channels in the 2400-2480MHz waveband. The reality, however, is that without mesh-like coverage in a given area, the effectiveness of this type of jamming is limited, especially given the fact that this approach blocks all types of Bluetooth broadcasts, and not just the FJA al-Qaeda transmissions.

In theory, because of the packet-driven nature of the Bluetooth piconets, it should be possible to narrowcast a version of a given FJA magazine that has malformed packets or headers. This would mean that, although the Bluetooth transmission would checksum and ACK/NAK as normal, when recipients try to view the magazine on their smartphones, the data would appear jumbled. In the longer term, given the firmware-updatable nature of modern smartphones, it should be possible to allocate MAC-like identification routines within Bluetooth packet headers – perhaps derived from the International Mobile Subscriber Identity (IMSI) of the smartphone's SIM card and/or the International Mobile Equipment Identity (IMEI) of the smartphone itself.

With most GSM and 3G networks now allowing only local SIM cards that have been identity-verified to use their networks, even if al-Qaeda uses stolen

or reprogrammed smartphones to seed the community with their jihadist narrowcasts, anyone receiving an e-magazine could trace the narrowcast back along its chain of transmission. At the very least, this would allow the intelligence agencies to cross-match the re-transmitters of the al-Qaeda Bluetooth transmissions with a list of known terrorists and, perhaps more importantly, identify probable supporters. In fact, since most cellcos now maintain active lists of the registration details of their pre-pay SIM cards, it is possible to cross-match the SIM cards of the re-transmitting smartphones and the time of the re-transmission with the triangulated location of the mobile at the time of the Bluetooth narrowcast. Through careful extrapolation of the available data, it then becomes possible to work out the probable location of the Class 1 Bluetooth al-Qaeda originator of a given e-magazine, and take action accordingly.

### About the author

*Steve Gold has been a business journalist and technology writer for 26 years. A qualified accountant and former auditor, he has specialised in IT security, business matters, the Internet and communications for most of that time. He is technical editor of Infosecurity and lectures regularly on criminal psychology and cybercrime.*

### Resources

- Bluetooth used for dating in Dubai. Youtube. Accessed Jul 2011.

<<http://www.youtube.com/watch?v=-HNS0SmzXXU>>.

- 'Member Suggests Using Bluetooth to Spread Terrorist Propaganda'. CBS News, 3 Jun 2008. Accessed Jul 2011. <[http://www.cbsnews.com/8301-502684\\_162-4148770-502684.html](http://www.cbsnews.com/8301-502684_162-4148770-502684.html)>.
- Stanley, Nigel. 'BBC Story on Bloor Research into Jihadists use of Smartphones'. Bloor Research, 26 Apr 2011. Accessed Jul 2011. <<http://www.bloorresearch.com/blog/Security-Blog/2011/4/bbc-story-on-bloor-research-into-jihadists-use-of-smartphone.html>>.
- Ackerman, Spencer. 'New Terror Propaganda Tool: Bluetooth'. Danger Room, Wired.com, 25 Jan 2011. Accessed Jul 2011. <<http://www.wired.com/danger-room/2011/01/bluetooths-beam-terror-propaganda-to-your-ear-drums/>>.
- Prucha, Nico. 'Entering a new dimension: Jihad via Bluetooth'. Jihadica, 24 Jan 2011. Accessed Jul 2011. <<http://www.jihadica.com/entering-a-new-dimension-%E2%80%93-jihad-via-bluetooth-part-1>>.
- 'Smart terror – terror Bluetooth'. Software. Noeman.org, 25 Sept 2009. Accessed Jul 2011. <<http://www.noeman.org/gsm/python-applications-s60v5-s60v3/91475-smart-terror-terror-bluetooth-beta-version-v-2-2-a.html>>.

# Beyond zero: analysing threat trends

Will Gragido, HP TippingPoint DVLabs

**In today's world of sophisticated and escalating cyber-attacks against vulnerable data, we have entered new and dangerous ground within the Internet threat landscape.**

In tracing the history of threats over the past decade, we saw a sharp rise in 'classic' threats between 2000 and 2005, which targeted systems that were widely

distributed across networks – such as the Microsoft Windows operating system. More sophisticated threats emerged in 2005 and 2006, indicating another level

of danger. And in 2008, with the advent of the Conficker worm, there appeared to be a resurgence of the 'classic' threat. In fact, Conficker was anything but ordinary or classic – it spread rapidly as variants were released into the mainstream.



Will Gragido