Cellphone *Risk Grows*

INNOVATIONS IN HAND-HELD DEVICES PROVIDE OPPORTUNITIES FOR CRIMINALS AND TERRORISTS

By *per Concordiam* Staff

The transformation of cellphones into powerful hand-held computers has revolutionized telecommunications, but has also produced security loopholes ripe for exploitation by criminals and extremists. Al-Qaida's formation of "mobile detachments" to spread jihadist recruitment videos via cellphones is just the start of it. Terror financiers have found it easier to transfer and launder money by simply punching a password into a cellphone keyboard. These all-purpose smartphones are also susceptible to hacking and tapping with the use of fraudulent cellphone applications or illicit receivers that can intercept calls within a certain radius.

It's all part of a process that Nigel Stanley, a widely quoted information technology security expert from England, describes as a "relentless cycle of new attacks and new innovations." The intimacy of such hand-held devices gives bad actors a chance to strike at a victim's vulnerable points anytime and anyplace. And for those liable to abuse it, inexpensive mobile phone technology can generate a large return for a small investment.

"Your smart/mobile phone certainly is a highly personal gadget, which is rarely shared – unlike family household computers," the terror-tracking website Jihadica.com wrote in March 2011. "The content on your mobile phone has a more private nature and allows you to quickly navigate and read through the jihadist materials without anyone noticing. The downside for jihadis, however, is an upside for the police, as the sympathizers are inspired to store incriminating content on their personal phones."

Triggering improvised explosive devices with cellphones, typically the disposable variety, has been a mainstay in the terrorist and criminal arsenal. But attacks can be much more subtle than that. Edward Gibson, a former FBI agent who provided IT security to the U.S. Embassy in London, said phone "apps," some downloaded innocently from Chinese sources, can turn cellphones into covert bugging devices. IT professionals have demonstrated how a makeshift base station, consisting of a $1,000 laptop computer and switchboard, can intercept cellphone signals from a particular radius without the caller's knowledge. Up to now, many of the targets have been corporate executives, but the vulnerability extends to government officials as well. Stanley pointed out that both U.S. President Barack Obama and British Prime Minister David Cameron are wedded to their hand-held devices.

A 2010 survey of 107 U.S. senior executives revealed that 61 percent reported monthly corporate security breaches due mainly to cellphone mishandling. Ponemon Institute, the firm that conducted the study, also investigated the prevalence of lost laptop computers. Ponemon learned in 2008 that business travelers in the U.S. and Europe lost 15,648 laptops a week, the leader in Europe being London's Heathrow Airport, with about 900 laptops lost weekly.

"A majority of business travelers say that their laptops contain confidential or sensitive information. However, most of these travelers admit they do not take steps to protect or secure the information contained on their laptop," Ponemon wrote, noting that Italian, Spanish and U.S. computer owners were the least security conscious.

Cellphones also disappear by the millions, though exact worldwide numbers are hard to come by. A 2005 government survey estimated the annual number of stolen cellphones in Great Britain at 700,000, many of which found their way to 46 foreign countries, the *Independent* reported. Even when the phones were

deactivated by their former owners, many still contained reams of personal data vulnerable to exploitation. To tackle the problem, Britain created a National Mobile Phone Crime Unit in 2003.

Gibson complained that corporate and government leaders, smitten with social media and other communications innovations, have lulled themselves into a false sense of security. People wouldn't tolerate an armed robber stealing millions from a bank vault, but they disregard larger thefts online. Criminals prey unceasingly on the public using domain names set up with phony names and addresses. Offshore servers, including one near the southeast coast of England on a concrete platform beyond the territorial reach of the British government, are available for use by law breakers. Cellphone signals are becoming easier to track using GPS, and a user's whereabouts easier to pinpoint using aerial mapping programs such as Google Earth. It's no time for people to grow complacent about cellphone and computer threats, Gibson warned during a speech at the London Counter Terror Expo in April 2011. "Technology has made us 'yes people,' " he said.

Recruitment tools sent via cellphones include jihadist how-to handbooks, religious literature and "snuff films" showing terrorists committing killings.

Jihadists have made inroads using these latest tools. Security experts reported that the Arab-language "Ansar Al-Mujahideen Forum" has been distributing jihadist mobile phone software since late 2009. It's part of al-Qaida's "mobile detachment" dedicated to reaching sympathizers within the broad Muslim public. Recruitment tools sent via cellphones include jihadist how-to handbooks, religious literature and "snuff films" showing terrorists committing killings. Sometimes the approach is less explicit. An Islamic dating subculture in which young men and women court each other clandestinely by cellphone provides an arena for exploitation, security experts say. "In some Arab countries, due to the harsh enforced segregation of the sexes, communicating and setting up 'secret dates' has mainly turned to the use of modern technology. AQ [al-Qaida] in its never-ending endeavor is also always keen to capitalize on newest technology," Jihadica.com wrote.

Terror financiers have adopted the practice of transferring money by cellphone, a method popular in much of rural Asia and Africa, where automated teller machines are scarce. Marrying that technology to the traditionally secretive Islamic money-lending system called *hawala* can make for a potent weapon. "Concerns have been raised about possible misuse of mobile technologies for criminal purposes," according to "Integrity in Mobile Phone Financial Services," a World Bank report. "Mobile phones are used by billions of people around the world to communicate, including criminals and terrorists. New mobile financial services may be susceptible."

Experts insist cyber defense must widen its scope to take in new, sophisticated cellphones. The era of the smartphone means powerful computers now fit in a user's palm, for good or evil. Users in Europe and Central Asia must take care, lest their personal portable devices be infected and turned against them, just as desktop computers are prone to attacks by viruses and malware. "Mobile phone jihad is a reality," Stanley said. "But the good news is there's a bunch of countermeasures to put in place." □

AGENCE FRANCE-PRESSE

A Saudi man checks his BlackBerry smartphone in Jeddah in 2010. Customers in Saudi Arabia and the United Arab Emirates faced service disruptions after authorities demanded that manufacturers provide access to encrypted messages sent on cellphones. The governments cited national security concerns.