RESEARCH PAPER

No. 131

MAY

2009

CELLS WARS:
The Changing Landscape of Communications Intelligence

Joseph Fitsanakis, PhD
(King College, Bristol, TN, USA)

Ian Allen
(Independent Consultant, Communications Interception Countermeasures Seoul, South Korea)

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)

 # 1, Kalavryton Street, Alimos, Athens, 17456, Greece

RIEAS URL:http://www.rieas.gr

RIEAS MISSION STATEMENT

Objective

The objective of the Research Institute for European and American Studies (RIEAS) is to promote the understanding of international affairs. Special attention is devoted to transatlantic relations, intelligence studies and terrorism, European integration, international security, Balkan and Mediterranean studies, Russian foreign policy as well as policy making on national and international markets.

Activities

The Research Institute for European and American Studies seeks to achieve this objective through research, by publishing its research papers on international politics and intelligence studies, organizing seminars, as well as providing analyses via its web site. The Institute maintains a library and documentation center. RIEAS is an institute with an international focus. Young analysts, journalists, military personnel as well as academicians are frequently invited to give lectures and to take part in seminars. RIEAS maintains regular contact with other major research institutes throughout Europe and the United States and, together with similar institutes in Western Europe, Middle East, Russia and Southeast Asia.

Status

The Research Institute for European and American Studies is a non-profit research institute established under Greek law. RIEAS's budget is generated by membership subscriptions, donations from individuals and foundations, as well as from various research projects. The Institute is autonomous organization. Its activities and views are independent of any public or private bodies, and the Institute is not allied to any political party, denominational group or ideological movement.

Dr. John M. Nomikos
Director

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)

Postal Address:

 # 1, Kalavryton Street
Athens, 17456, Greece
Tel/Fax: + 30 210 9911214

E-mail: **rieas@otenet.gr**

Chrysanthos Lazaridis, Diktyo (Network) 21

Meir Javedanfar (PhD), Middle East Economic-Political Analysis Inc.

Nick Larigakis, Director, American-Hellenic Institute

Daniele Ganser (PhD), Basel University

Prof. Siegfried Beer (PhD), Director, Austrian Centre for Intelligence, Propaganda and Security Studies

Prof. Herman Matthijs (PhD), Free University of Brussels

Christopher Deliso (MPhil), Balkan security & politics analyst & Director, Balkanalysis.com

Prof. Michael Wala (PhD), University of Munich

Prof. Wolfgang Krieger (PhD), University of Marburg

Michael Tanji, Director at Threatswatch.org - (OSINT)

Prof. Ioannis Mazis (PhD), Ionian University

Robert Nowak (PhD Cand), Institute of History of the Polish Academy of Sciences, Bureau of the Committee for Special and Intelligence Services (Prime Minister's Chancellery)

Lauren Hutton (PhD), Researcher, Institute for Security Studies (South Africa)

LTC General, Prof. Iztok Podbregar (PhD), University of Maribor, Former National Security Advisor to the President of the Republic of Slovenia, Former Chief of Defense (CHOD), Former Director of the Slovenian Intelligence and Security Agency, Former Secretary of the Slovenian National Security Council.

Prof. David Wright- Neville (PhD), Global Terrorism Research Centre, Monash University (Australia)

Research Associates

Ioannis Konstantopoulos (PhD), Intelligence Studies
Liam Bellamy (MA), Maritime Security (Piracy)
Spyridon Katsoulas, (PhD Candidate) Greek-American Relations
Ioannis Kolovos (MA), Illegal Immigration in Greece
Naveed Ahmad (MA), South-Central Asia and Muslim World
Ioannis Moutsos (MA), Independent Journalist
Nadim Hasbani (MA), Lebanon-Syria and North African States
Nikos Lalazisis (MA), European Intelligence Studies

RESEARCH PAPER

No. 131

MAY

2009

CELLS WARS:
The Changing Landscape of Communications Intelligence

Joseph Fitsanakis, PhD
(King College, Bristol, TN, USA)

Ian Allen
(Independent Consultant, Communications Interception Countermeasures
Seoul, South Korea)

Abstract:

The 2008-2009 Israel-Gaza conflict featured a series of innovative approaches to communications intelligence, which included utilizing civilian telephone networks to achieve tactical and psychological objectives. The "cell war" between the IDF and Hamas is indicative of an ongoing global struggle between asymmetrical insurgents and state actors to control large-scale telecommunications structures. "Cell wars" have been taking place for quite some time in Iraq, Somalia, Afghanistan, Lebanon, Syria, and several other nations, including inside the United States. Weapons in this hi-tech conflict include surveillance satellites, voice scramblers, encryption software and mobile phone cameras, among other technologies. Essentially, this war is being fought over the control over national and international telecommunications grids, and centers increasingly on telecommunications service providers — companies such as Jawwal in Palestine, Roshan in Afghanistan, or Mobilink in Pakistan. These companies are rapidly becoming combat zones in a battle to control the channels of digital communications in 21st-century asymmetrical warfare.

Cell Wars:
The Changing Landscape of Communications Intelligence

From December 27, 2008, until January 18, 2009, the world witnessed yet another violent confrontation between Israel and the Palestinians. From its very beginning, the 2008-2009 Israel-Gaza conflict, as it has come to be known, displayed the familiar aspects of political controversy and military brutality that typify the long history of the Israeli-Palestinian rivalry. Tactically, however, the Israeli military's incursion into the Gaza strip (codenamed Operation CAST LEAD) featured a series of innovative

approaches to urban asymmetrical warfare, which, some observers claim, enabled the Israeli Defense Forces (IDF) "to outflank and defeat [Palestinian group] Hamas in its own territory" (Eshel 2009).

At the center of these new tactics was the "unprecedented level of interservice cooperation" (*ibid*.) between the IDF and Israel's Internal Security Agency (ISA). Throughout the 23-day conflict, agents of the ISA, Israel's foremost domestic intelligence organization, which is also known as *Shabak*, or *Shin Bet*, were reportedly embedded in Israeli command posts and forward units deep into the Gaza Strip. The IDF utilized advanced information and communication technologies to "rapidly [turn intelligence leads gathered by ISA agents] into targeting data for strikes against time-critical targets" (*ibid*.).

What was novel from a communications intelligence point of view was that both landline and cellular networks in the Strip were intensely targeted by the IDF-ISA operational interface. Moreover, the two agencies appear to have utilized the Gaza's telephone network to achieve both tactical and psychological objectives. This innovative approach partly explains why the Israeli forces refrained from sabotaging Gaza's telephone network during the incursion. Some parts of the network in northern Gaza suffered damage during IDF raids (Anon 2008a), but such instances appeared to be inadvertent. In fact, the Strip's telecommunications network was primarily disabled from being swamped by "intense calls between people during the hours of shelling" (*ibid*.), rather than out of deliberate targeting by the IDF. There were reports on as late as January 13, five days before the end of mass hostilities, of civilian telephones in Gaza that "didn't stop ringing during the day and receiving different phone calls" (Ramadan 2009), signifying an essentially functioning telecommunications system. This was augmented during the conflict by the executive decision by Jawwal, the sole Palestinian cellular telecommunications service provider, to donate airtime credit to its subscribers, thus allowing them to continue to use their cellular telephones amidst the chaos of the conflict (Estrin 2009).

THIS IS THE IDF CALLING

Long familiar with IDF and ISA surveillance tactics, the primarily young, cell-phone-savvy population of the Gaza Strip was acutely aware of the primary reason why the Strip's telephone network was left standing during the conflict. In the words of Amman Aked, Jawwal's director in Ramallah, the motive was "to make sure that the militant people actually use their [cell] phones and [the Israeli forces] can look at their locations" (*ibid*). But another, equally important, reason soon became apparent: on January 7, 2009, Israel's Ministry of Foreign Affairs voluntarily revealed that, in the early hours of the conflict, the IDF placed "around 20,000 phone calls throughout [*sic*] the entire Gaza Strip", including "10,000 phone calls [...] to the residents of Rafah" alone (Anon 2009a). The calls relayed a pre-recorded warning in Arabic that "the life of anyone in whose home ammunition and weapons are to be found is in danger, and he must leave the place for the sake of his own safety and that of his family" (*ibid*).

The frequency of these phone calls intensified during the main phase of the Israeli incursion. Many Gazans reported receiving "unusual phone calls" on both cellular and landline networks, prompting them to supply the identities of Hamas militants or giving them a few minutes to evacuate their homes prior to the arrival of armed Israeli helicopters (Ramadan, 2009; Rabinovich, 2008; 2009; Michaels, 2009). In virtually every case, the male Arabic-speaking caller clearly identified himself as a member of the IDF (Rabinovich 2008), while in nearly all cases the telephone calls were routed through international network carriers (Michaels 2009).

IDF officials suggested that the telephone calls were placed as "a service" to the Palestinians, "[t]o reduce civilian casualties" in Gaza and "to warn civilians [...], especially when we're going to target a building" (Rabinovich, 2009; Michaels, 2009). However, the nature of many of the calls suggests multifaceted motives that incorporate significant intelligence components. In January, Israeli officials confirmed to *The New York Times* that "Israeli intelligence officers [were] telephoning Gazans and, in

good Arabic, pretending to be sympathetic Egyptians, Saudis, Jordanians or Libyans" (Erlanger 2009). Palestinian cellular telecommunications service provider Jawwal reported that on January 15 at least 1,500 subscribers contacted the company's customer service center in Ramallah to "complain about suspicious calls from abroad" (Estrin 2009). Many subscribers reported that, after expressing support for Hamas, the foreign callers typically asked for specific information regarding "local conditions, whether the family supports Hamas and if there are fighters in the building or the neighborhood" (Erlanger 2009). Several sources confirmed that a number of Arab- and Muslim-owned telephone service providers in Libya, Yemen, Saudi Arabia, Sudan, Australia and elsewhere, offered their customers free calls to the Gaza strip in a concerted expression of solidarity with the Palestinian population (Ramadan, 2009; Estrin, 2009). But complimentary solidarity calls accounted for only a portion of the remarkable 30% jump in international calls to the Gaza Strip during the Israeli incursion (Estrin 2009). The Israeli piggybacking tactic caused Jawwal to consider ways of blocking the suspicious calls, which apparently kept coming in at all times of the day or night (Ramadan 2009). But the Palestinian cellular service provider eventually realized it would be impossible to selectively block what were essentially untraceable international calls (Estrin 2009).

RECENT PRECEDENTS

The 2008-2009 Israel-Gaza conflict was not the first time that the Israeli military-intelligence complex targeted another country's telephone network in pursuit of both tactical and psychological objectives. During the 2006 Israel-Gaza conflict (June 28-November 26), there were isolated reports of "a new Israeli tactic of using telephone, radio and leaflets to warn Gazans of impending attacks" (Urquhart, 2006). One family in Gaza City received a telephone call from an individual identifying himself as "Danny [...], an officer in Israeli military intelligence", who informed them that "[i]n one hour [the IDF] will blow up your house". Approximately an hour after the call, an Israeli helicopter fired missiles at the house (*ibid*). Noting that the IDF's warnings often turned out to be misleading, the Palestinian Center for Human Rights described the tactic as a malicious form of "psychological warfare". In one instance, a family in central Gaza's densely populated Bureij refugee camp received a call from a woman identifying herself as an "Israeli intelligence officer", who told them their home would soon be targeted by the IDF and should be evacuated immediately. An hour later, the woman called back to inform the family she had "made a mistake" and politely terminated the call by prompting the family to "be safe" (*ibid*).

In July of 2008, Lebanon's Ministry of Telecommunications notified the United Nations of a series of seemingly random calls placed by Israeli intelligence on unsuspecting Lebanese telephone subscribers in the days following the July 16, 2008 prisoner swap between Israel and Lebanese organization Hezbollah. The Ministry said the calls relayed a pre-recorded message from "the state of Israel", promising "harsh retaliation" against any planned attacks by Hezbollah and denouncing what it called Hezbollah's efforts to create "a state within a state" in Lebanon. Lebanese Minister of Telecommunications, Jibran Bassil, said Israeli intelligence had engaged in similar practices during the 2006 Lebanon War, but refused to elaborate (Karam 2008).

In late October 2008, reports emerged from Syria about a "barrage of recorded phone messages asking people for information about missing Israeli soldiers in exchange for a $10 million reward". According to a source inside the government-owned Syrian Telecommunications Establishment, the calls were in Arabic and were received by "thousands of landline subscribers", who were prompted to dial either of two telephone numbers beginning with 44, the international calling code for Britain. Syrian government and security sources alleged the telephone calls were "designed to recruit agents to work for Israeli intelligence" (Anon 2008b).

THE BROADER CONTEXT

In essence, the Israeli telephone operations outlined above, represent the most recent military and intelligence response to a number of communications challenges in modern asymmetrical warfare. These challenges are produced by the combination of three strategically interrelated factors: first, the rising physical and social mobility of transnational asymmetrical actors (Sageman, 2004, p.139ff); second, the unprecedented growth of cellular telecommunications networks in the global south (Hanson 2007, p.125ff); third, the interface between increasingly mobile, increasingly networked asymmetrical actors, and increasingly pervasive cellular telecommunications.

This situation is apparent in Iraq, where US forces have been fighting a well-organized insurgency since 2003. To a large extent, the insurgents' heavy use of cellular phones and the Internet accounts for the widely recognized fact that, in the words of General John Abizaid, former Commander of the US Central Command, "[t]his enemy [in Iraq] is better networked than we are" (Shachtman 2007). In light of this fact, it is somewhat ironic that the US occupation forces recognize the social and economic importance of developing Iraqi telecommunications (Braude 2003, p.110-112) while understanding that "[e]very new cell tower means a hundred new nodes on the insurgent network" (Shachtman 2007). By 2007, the utilization of the Internet by young members of Iraqi insurgent groups was so widespread, that the location of every Internet *café* in Baghdad was among targets displayed in the US armed forces' Command Posts of the Future (CPOF) system, a digital monitoring grid guiding military operations in the country (*ibid*). In the early days of the insurgency, resistance groups responded to the Americans' surveillance of cell phone networks by systematically destroying local cell towers (*ibid*). More recently, however, the insurgents have shown clear signs of having mastered the principles of asymmetrical communications, and are now even considering using the video capabilities of third generation cellular devices for "monitoring enemy activities" and "in tandem with conducting attacks" (Anon 2008c).

Somalia offers another example of an active insurgency that is rapidly mastering the asymmetrical benefits of cellular telecommunications. In late 2006, the US approved and assisted Ethiopia's invasion of Somalia in what is in fact one of America's most recent covert wars. The operational aim of the invasion was to obliterate the local grassroots leadership of the Islamic Courts Union (ICU) and prevent the solidification of its rule in the country. Soon after the Ethiopian invasion, rank-and-file members of the ICU went underground in an attempt to organize a guerilla war against the invaders. Arguably, the most militant segment of the new underground movement is *al-Shabaab* (The Party of Youth), which used to be the youth organization of the pre-invasion ICU (Fitsanakis 2009). The strength of *al-Shabaab* and other *al-Qaeda*-linked militant groups in Somalia has reportedly been increased by what one informed observer has termed the severe blowback of the US secret rendition program in the country (Salopek 2008). Recent reports state that *al-Shabaab's* middle leadership receives its operational instructions from the organization's commanders, referred to as "emirs", via daily text messages or phone calls placed from remote locations in Somalia and abroad (Mohamed 2009). It is also reported that the group's members are routinely "given prepaid phone cards to carry out their day-to-day operations", which include sending threatening text messages to "those *al-Shabab* believes oppose them" (*ibid*).

But the most pertinent illustration of the growth of guerilla communications in asymmetrical insurgencies is undoubtedly to be found in rural Afghanistan, as well as in Pakistan's northwestern Federally Administered Tribal Areas. Cellular telephony was virtually unknown in Taliban-ruled Afghanistan, and was gradually introduced following the 2001 US invasion. By 2008, cellular devices had reportedly become "the most popular way of communicating" in the country (Brain 2008), with cellular phone coverage extended over virtually the entire country (Stuart 2008). In 2003, when Roshan, Afghanistan's largest cellular telecommunication service provider —and the country's largest investor,

employer and taxpayer— was founded, its Chief Executive Officer, Karim Khoja, exclaimed that his customers "may be Taliban, they may be warlords, who cares? We are apolitical —they are customers". He added that "everybody in Afghanistan, including the Taliban, understands the importance of being able to communicate" (Anon 2007a). But Mr. Khoja's convivial gesture to the Taliban concealed a less welcoming side: Western countries, which were among Roshan's most enthusiastic investors, hoped to lure the Taliban into the cellular culture, so that their communications could be intercepted by Western intelligence agencies.

NATO and Coalition forces are currently employing a similar method in Pakistan's Federally Administered Tribal Areas. In March of 2009, Mobilink, Pakistan's premier cellular telecommunications service provider, announced the start of its cellular coverage in South Waziristan, after having recently done the same in Bajaur, Mohmand, Kyber and Kurram. Pakistani newspaper *The Daily Times* reported that the region's Taliban forces have initially "welcomed the facility". Security sources told the paper that "use of electronic telecommunication equipment by the Taliban has helped security agencies nab wanted men in the past", and added that "[t]his is what we hope happens" in South Waziristan as well (Anon 2009b).

VOICE SCRAMBLERS, PRIVATE NETWORKS AND VOIP

In Afghanistan, however, the Taliban have begun to realize that, in the words of one of their spokesmen, "the US and other foreign troops in the country are using mobile phone signals to track down the insurgents and launch attacks against them" (Page 2008). They have therefore started to accuse Rochan and other cellular telecommunications service providers of "colluding with US and other forces" (Brain 2008). In February of 2008, they gave cellular service companies 72 hours "to stop their signals from 5 p.m. to 3 a.m. in order to stop the enemies from getting intelligence through mobile phones and to stop Taliban and civilian casualties" (Shachtman 2008). The Taliban said that if the companies failed to abide their cell masts and offices would be targeted (Page 2008).

One observer has speculated that the Afghan Taliban are attempting to eliminate institutional cellular service providers from the frequency spectrum in order to launch their own private cellular networks in areas under their control (Page 2008). If this materializes, it will not be the first time. In Lebanon, Hezbollah has been operating its own private telecommunications network since at least 2007. In August of that year, Lebanon's Minister of Telecommunications described the organization's independent communications infrastructure as "a state violation" that subverted the authority of the Lebanese authorities and "went beyond logic". But Hezbollah sources responded that the group required its own telecommunications network in the south "to protect its members from Israeli attacks and assassinations" (Anon 2007b).

In reality, advanced satellite-based communications interception systems are able to pick up cellular signals even from private telecommunications networks —that is, without assistance from service providers. But by maintaining its own private network, an insurgent force can add a small stumbling block to the interception process, which can be further frustrated by additional technical features such as voice scramblers, strong encryption, voice-over-Internet-protocol (VOIP) capabilities, or a combination of all three. VOIP systems are already posing severe problems for intelligence agencies targeting asymmetrical insurgencies. The distinguishing feature of VOIP-based communications, which form the technical basis of popular communications software such as Skype and Vonage, is that audio signals are digitized and travel through most of the Internet infrastructure in binary, rather than audio, format. Furthermore, they are often encrypted using algorithms of various strengths. Additionally, VOIP data packets travel through Internet networks looking for unused lines, which may not necessarily constitute the most direct route to a given destination. Consequently, a VOIP source signal from New York to Los Angeles could easily reach its destination through, say, Reykjavik or Bogota. What is more, binary data packets often split, with different parts following different routes

to a given destination, only to reunite at a switch close to the end destination. This poses severe barriers to authorized communications interception, as well as to the ability of law enforcement and intelligence agencies to locate the source of target calls (Allen 2008). As early as 2005, there were reports describing Internet-based audio communications as a "massive technological blind spot" troubling US government wiretap experts (Bennett 2005). More recently, an anonymous industry insider alleged that the US National Security Agency (NSA) is actively soliciting several companies in its search for a way out of the technical challenges posed by Skype's strong encryption and peer-to-peer network architecture. The unnamed source claimed that NSA is "offering billions to any firm which can offer reliable eavesdropping on Skype IM and voice traffic [...]. They are saying to the industry, you get us into Skype and we will make you a very rich company" (Page 2009). The popularity of VOIP systems has also been identified by Sir David Pepper, director from 2003 to 2008 of Britain's General Communications Headquarters (GCHQ), as a threat that is "seriously undermining his organization's ability to intercept communications" (Owen 2008).

In the meantime, many Taliban insurgents in Afghanistan are already using Skype for their internal communications, in efforts "to evade detection by MI6", Britain's external intelligence agency (*ibid*). And they are not alone. In November 2008, while carrying out their three-day attack on Mumbai, India, members of the Pakistani militant group *Lashkar-e-Taiba* used VOIP-enabled mobile devices to communicate with their handlers in Pakistan. They remained in telephone contact with them throughout the operation, receiving real-time instructions and encouragement, until they either committed suicide or were shot dead by Indian security forces (Kahn 2008). After studying the technical aspects of the attack, the New York Police Department concluded that shutting down cellular and other wireless communications over an entire area would be the only feasible method of disrupting mobile VOIP contact between members of an asymmetrical cell and their handlers during an operation (Miller 2009).

ASYMMETRIC INSURGENCIES FIGHT BACK

It is not clear how the inevitable growth of encrypted telecommunications, as well as VOIP systems, will affect the ability of intelligence agencies to penetrate the communications systems of asymmetric insurgencies. In places like the Gaza Strip, it is apparent that the IDF are currently able to penetrate Palestinian telecommunications networks at will. They do this through a combination of routine collection of open source or dialing data (in the case of landline subscribers, whose telephone numbers are "generally available in phone books" [Michaels 2009]), as well as intelligence infiltration of cellular telecommunication service providers. This would not be particularly arduous in the Gaza Strip or the West Bank, where "all the important connections and the international telecommunication systems are connected in areas located outside the Palestinian territories" and where "inner-city, long distance, and international connections are still physically and financially under the Israeli control" (Faour 2007).

Nevertheless, even under severe penetration of their telecommunications infrastructure by enemy intelligence, asymmetrical insurgencies have amply demonstrated that they are not mere passive targets of communications intelligence. During the 2008-2009 Israel-Gaza conflict, there were numerous instances of civilians refusing to abide by the IDF telephone call directives to evacuate their homes. In several cases, residents climbed up to the roofs or their homes and defiantly remained in plain view of hovering Israeli aircraft, thus managing to prevent impending airstrikes (Rabinovich 2009). On January 1, 2009, Israeli media reported that dozens of Israeli mobile phone subscribers received text messages from Hamas "warning them that the offensive in Gaza will only bring about massive rocket fire on Israel" (Waked 2009). Less than a week later, a similar psychological operation by Hamas specifically targeted mobile phones belonging to Israeli reserve soldiers. The Palestinian group sent numerous fictitious "emergency call for duty" text messages to Israeli reservists, ordering them to present themselves at an IDF enlistment center in Haifa (Goren 2009). One of the young Israelis who received a text message from Hamas described the "unnerving" feeling he experienced, noting that "[i]t feels like they've invaded you" (Michaels 2009). To prevent intimidation and confusion

among the ranks of the IDF, Israeli military leaders forbade soldiers to carry personal cellular devices with them in the field (*ibid*). This was in sharp contrast to the 2006 Lebanon War, when "Israeli soldiers commonly tucked their phones into their cargo pockets when they went onto the battlefield and regularly used them to call home or keep in touch with friends" (*ibid*). According to Israeli retired brigadier general Shlomo Brom, Hezbollah intelligence officers took advantage of the Israeli soldiers' attachment to their cell phones by regularly eavesdropping on their conversations (*ibid*).

AT THE CENTER OF THE STORM

Even in Israel's heavily penetrated occupied territories, as the volume of telephone usage continues to increase by over 50% per year (Anon 2007c), as the cost of cellular service provision continues to decline, and as the asymmetrical communication skills of the insurgents improve, organizations such as Hamas and Fatah will undoubtedly consider going the way of Hezbollah and establishing their own independent communications infrastructures. Moreover, their technical dependency on Western hardware providers (Anon 2002) could well diminish in favor of providers from friendly regimes, such as Syria or Iran.

The move toward establishing independent communications infrastructures is not unique to insurgencies, or even to developing nations. The present authors have been aware since 1998 of organized efforts by large criminal cartels or adversary intelligence organizations in the United States to purchase locally based telecommunications service providers in order to shelter their communications from government surveillance. One security expert of a large US telecommunication carrier told one of the authors in 2001:

in effect —I've made this comment to the [Federal] Bureau [of Investigation (FBI)] that I'm sure they were well aware of [...]— who is to say that drug dealers or the mob cannot go out and create their own —or have not gone out and created their own— competitive local exchange carrier? They can do that themselves. I am sure they have thought of that. It would take a lot of financial resources to do that, but you're talking about folks that have strong financial backing. They launder a lot of stuff [Fitsanakis 2001].

Commenting on this issue, an FBI Special Agent revealed to one of the authors that the Bureau has discovered at least one case where a local exchange carrier was purchased by organized criminal interests wishing to communicate in a surveillance-free environment:

[w]e've actually seen the Mafia —the Italian Mafia— purchase a telephone company in New Jersey —the whole telephone company. Now, how are we going to tell that? You can't just knock on the door and say "we've got this [electronic surveillance] court order and we were wondering if you could help us, but don't tell anybody" [Fitsanakis 2000].

The above developments may be pointing to a rapidly changing landscape in communications intelligence, in which asymmetrical actors reinvent cellular telecommunications networks to achieve operational objectives. At the same time, state intelligence agencies are being drawn into viewing civilian telecommunications networks as operational assets to be utilized in the interests of promoting tactical or psychological goals. Regardless of the successes or failures of participating actors, both approaches appear to compete for control of telecommunications providers, who are finding themselves progressively closer to the center of the storm. By virtue of their critical role in administering large-scale communications grids, these providers will continue to become the targets of overt and covert, legitimate and illegitimate operations to control large-scale telecommunications grids. These operations will often include political and physical threats, blackmail, intimidation, and even murder, as many observers seem to believe was the case in Greece's 2005 Vodaphone and Italy's 2006 Telecom Italia wiretapping scandals (Klein & Pontoniere, 2006). Ultimately, in this early stage of the changing landscape of communications intelligence, control over the medium, and not the content, of communications will be the primary operational goal.

REFERENCES CITED:

Allen, I. (2008) Hi-Tech Mumbai Attacks Pose Forensics Problems for Intel Agencies, *intelNews*, 09 December, available online at: http://intelligencenews.wordpress.com/2008/12/09/01-15/

Anon. (2002) Telecommunications in the Palestinian Authority Areas, *African & Middle Eastern Telecom*, 49(3), Brighton, MA, September, p11.

Anon. (2007a) Shining a Light, *The Economist*, 08 March, available online at: http://www.economist.com/people/displaystory.cfm?story_id=8810

Anon. (2007b) Lebanese Minister Slams Hezbollah Telephone Network, *Ha'Aretz*, 29 August, available online at: http://www.haaretz.com/hasen/spages/898840.html

Anon. (2007c) West Bank and Gaza, *ICT At A Glance*, (Washington, DC: The World Bank).

Anon. (2008a) Gaza Telecommunications Network Damaged by Israeli Raids, The Independent Commission for Human Rights, Ramallah, 30 December, available online at: http://www.ichr.ps/etemplate.php?id=95

Anon. (2008b) Strange Israeli Phone Calls Alarm Syrians, *Syria News Briefing*, 04 December, available online at: http://www.middle-east-online.com/english/?id=29082=29082&format=0

Anon. (2008c) Sample Overview: al-Qaida-Like Mobile Discussions and Potential Creative Uses, Open Source Intelligence Team, 304th Military Intelligence Battalion, United States Army, 16 October [copy on file with authors].

Anon. (2009a) IDF Issues Warnings to the Civilians of Gaza, Israeli Ministry of Foreign Affairs, 07 January, available online at: http://www.mfa.gov.il/MFA/Government/Communiques/2009/IDF_warns_Gaza_population_7-Jan-2009.htm

Anon. (2009b) Cellular Company Launches Service in South Waziristan, *The Daily Times*, 24 March, available online at: http://www.dailytimes.com.pk/print.asp?page=2009\03\24\story_24-3-2009_pg7_22

Bennett, B. (2005) Psst! The FBI Is Having Trouble on the Line, *Time*, 10 August, available online at: http://www.time.com/time/printout/0,8816,1090908,00.html

Brain, J. (2008) Taleban Issue Mobile Phone Threat BBC, 25 February, available online at: http://news.bbc.co.uk/2/hi/south_asia/7262519.stm

Braude, J. (2003) *The New Iraq: Rebuilding the Country for Its People, the Middle East and the World* (New York, NY: Basic Books).

Erlanger, S. (2009) A Gaza War Full of Traps and Trickery *The New York Times*, 11 January, available online at: http://www.nytimes.com/2009/01/11/world/middleeast/11hamas.html

Eshel, D. (2009) New Tactics Yield Solid Victory in Gaza, *Aviation Week*, 11 March, available online at: http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/GAZA031109.xml

Estrin, D. (2009) Cell Phone Help for Gaza, *The World*, Public Radio International, 16 January, available online at: http://www.theworld.org/node/23892

Faour, Z. (2007) The Information Technology Future of the State of Palestine, *Information Technology Landscape in Nations Around the World*, Kogod School of Business, American University, Washington, DC, available online at: http://www.american.edu/initeb/zf4862a/palestin.htm

Fitsanakis, J. (2000) Interview with a member of the Telecommunications Industry Liaison Unit, CALEA Implementation Section, US Federal Bureau of Investigation, Atlanta, GA, 15 November [interview transcript on file with author].

Fitsanakis, J. (2001) Interview with technical project manager of a large US telecommunication carrier, Atlanta, GA, 15 June [interview transcript on file with author].

Fitsanakis, J. (2009) FBI Probed Obama Inauguration Threats by Somali Militant Group, *intelNews*, 21 January, available online at: http://intelligencenews.wordpress.com/2009/01/21/01-52/

Goren, Y. (2009) IDF Reserve Troops Receive Fictitious Calls for Duty in Gaza, *Ha'aretz*, 08 January, available online at: http://www.haaretz.com/hasen/objects/pages/PrintArticleEn.jhtml?itemNo=1053580

Hanson, J. (2007) *24/7: How Cell Phones and the Internet Change the Way We Live, Work, and Play* (Westport, CT: Praeger).

Kahn, J. (2008) Mumbai Terrorists Relied on New Technology for Attacks, *The New York Times*, 09 December, available online at: http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html

Karam, Z. (2008) Freed Lebanese say they will keep fighting Israel, The Associated Press, 17 July, available online at: http://www.beiruttimes.com/site2/index.php?subaction=showcomments&id=1216308317

Klein, J. & Pontoniere, P. (2006) Security Experts' 'Suicides' Called into Question: European Media Probe Dangers of Secret Surveillance Systems, *New America Media*, 16 August, available online at: http://news.newamericamedia.org/news/view_article.html?article_id=d54bf5a301e73cbba0663d69a33d80c0

Michaels, J. (2009) Cellphones Put To 'Unnerving' Use in Gaza, *USA Today*, 13 January, available online at: http://www.usatoday.com/tech/wireless/2009-01-13-gazaphones_N.htm

Miller, J. (2009) NYPD Eyes Disrupting Cell Phones in Event of Terrorist Attack, Fox News, 08 January, available online at: http://www.foxnews.com/politics/2009/01/08/nypd-interrupt-cell-phone-service-event-terrorist-attack/

Mohamed, M. (2009) Somalia's Text Message Insurgency, BBC, 16 March, available online at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/africa/7932316.stm

Owen, G. (2008) Taliban Using Skype Phones to Dodge MI6, *The Daily Mail*, 13 September, available online at: http://www.dailymail.co.uk/news/worldnews/article-1055611/Taliban-using-Skype-phones-dodge-MI6.html

Page, L. (2008) Taliban Demand Night-Time Cell Tower Shutdown, *The Register*, 25 February, available online at: http://www.theregister.co.uk/2008/02/25/taliban_cell_tower_prohibition/

Page, L. (2009) NSA Offering 'Billions' for Skype Eavesdrop Solution, *The Register*, 12 February, available online at: http://www.theregister.co.uk/2009/02/12/nsa_offers_billions_for_skype_pwnage/

Rabinovich, A. (2008) Israel Warning Civilians to Flee, *The Australian*, 30 December, available online at: http://www.theaustralian.news.com.au/story/0,25197,24853989-15084,00.html

Rabinovich, A. (2009) Nuclear Fear Drives Israel's Hard Line, *The Australian*, 03 January, available online at: http://www.theaustralian.news.com.au/story/0,25197,24867840-601,00.html

Ramadan, S.A. (2009) Telephone, An Only Means of Communication with Gazans, Xinhua News Agency, 13 January, available online at: http://news.xinhuanet.com/english/2009-01/13/content_10653165.htm

Sageman, M. (2004) *Understanding Terror Networks* (Philadelphia, PA: University of Pennsylvania Press).

Salopek, P. (2008) Renditions Fuel Anger Against US, *The Chicago Tribune*, 04 December, available online at: http://www.chicagotribune.com/news/nationworld/chi-shadow_war3dec04,0,7830347,print.story

Shachtman, N. (2007) How Technology Almost Lost the War, *Wired*, 15.12, 27 November, available online at: http://www.wired.com/print/politics/security/magazine/15-12/ff_futurewar

Shachtman, N. (2008) Taliban Threatens Cell Towers, *Wired*, 25 February, available online at: http://blog.wired.com/defense/2008/02/in-iraq-when-th.html

Stuart, R. (2008) Cell Phones Connect Afghans to Rest of World *Morning Edition*, National Public Radio, 26 February, available online at: http://www.npr.org/templates/story/story.php?storyId=19357336

Urquhart, C. (2006) The Call That Tells You: Run, You're About To Lose Your Home and Possessions, *The Guardian*, 28 July.

Waked, A. (2009) Hamas Sends Text Messages to Israeli Cell Phones, *YNet News*, 01 January, available online at: http://www.ynetnews.com/articles/0,7340,L-3648799,00.html.

About the Author:

Dr. Joseph Fitsanakis is teaching at the King College, Bristol, TN, USA, and Mr. Ian Allen is an Independent Consultant, Communications Interceptions Countermeasures, Seoul, South Korea)

RIEAS Publications:

RIEAS welcomes short commentaries from young researchers/analysts for our web site **(about 700 words),** but we are also willing to consider publishing short papers (**about 5000 words**) in the English language as part of our publication policy. The topics that we are interested in are: transatlantic relations, intelligence studies, Mediterranean and Balkan issues, Middle East Affairs, European and NATO security, Greek foreign and defense policy as well as Russian Politics and Turkish domestic politics. Please visit: **www.rieas.gr (Publication Link)**