

TOO MANY TERRORISTS SPOIL THE PLOT

Dr. Gordon Woo

Risk Management Solutions

Gordon.Woo@rms.com

INTRODUCTION

Consider a terrorist network actively planning a number of major terrorist attacks against the US homeland. Depending on which nodes in the hierarchy are removed by counter-terrorism forces, the attack plans can be disrupted to a greater or lesser extent, forcing them to be delayed, or perhaps abandoned if certain critical nodes are taken out. According to the assumptions made on the network structure, and the node removal process, the probability of plan disruption can be calculated using combinatorics (Farley, 2003). Increasing the number of terrorists actively involved enhances the redundancy and hence the resilience of attack plans. Even the removal of a large number of nodes may yet leave intact pathways for operations to be executed, notwithstanding significant network impairment.

Apart from resilience against node loss, there are other terrorist concerns. Gunther and Hartnell (1978) have considered the fear of betrayal. From studying the diverse ways in which Al Qaeda operatives have been found, (and corroborated by the lack of response to the bounties offered for senior Al Qaeda figures), betrayal is comparatively rare within close-knit Jihadi communities. In this paper, terrorist attack planning is analyzed from another perspective. Involvement of more operatives increases personnel redundancy, but also the chance is increased of the planning process being unwound through forced disclosure by operatives during interrogation; from decryption of data on their computers; and from tracking down their real and virtual contacts. The greater the number of operatives involved in attack planning, the greater is the chance that the plans will unravel due to operative indiscretion and effective counter-terrorism surveillance and data-mining. This is one of the principal factors limiting the risk of a nuclear terrorist attack, which would require a large team of skilled technicians. Too many terrorists can spoil the plot. But how many is too many?

In May 2001, months before 9/11, Osama bin Laden addressed the Al Farouq military training camp near Kandahar in Afghanistan (Bell, 2005), and proclaimed that there were *'Fifty men willing to bear their souls in their hands for the Jihad to attack America'*. Why only fifty? Why not a hundred, or two hundred? Thousands of Mujahidin had already been trained and prepared for martyrdom missions. In his many public messages to the world¹, Osama bin Laden has made clear his sacred quest to see the world's superpower humbled, and his belief that the USA could be defeated, as were the Soviets. Having declared a Jihad against the Americans occupying his homeland of Saudi Arabia,

¹ See for example the compilation by Lawrence, 2005

why not deliver the maximum economic blow in 2001, when the crucial element of surprise was very much in Al Qaeda's favor?

It is shown here that, from the perspective of a prudent terrorist operations manager, fifty is about the maximum number of Jihadis who could have been sent on a wave of attacks beginning on 9/11. Intuitively, Osama bin Laden would have figured out that launching a greater number of Jihadis in attack waves against the US in 2001 would have been unnecessarily foolhardy and risky - and unduly impatient. Patience is deeply rooted in Islam. Indeed, patience is half of the Islamic concept of faith, that covers action, (for which gratitude is due to Allah), and abstinence from action, (for which patience is demanded). It is now known that, earlier in the planning stage for 9/11, the idea of flying planes into West Coast skyscrapers was considered by Al Qaeda. But such extra complexity and audacity were scaled back. It is a counterfactual conjecture that had the 9/11 operation been twice as ambitious, Mohammed Atta and the other hijackers might be in jail now, and the World Trade Center might still be standing.

As it was, even with the plot in its more moderate final four plane realization, Al Qaeda rode their luck and had some close escapes. Following a National Security Agency (NSA) communication intercept, Nawaf Al Hazmi and Khalid Al Midhar, two of the Pentagon-bound AA77 hijackers, were known by the CIA to have met in Malaysia. The two Saudis were placed on the TIPOFF watch-list on August 24, 2001, but this was too late to track them in the USA in time. The pilot of UA93 also had a narrow escape. On September 8, Ziad Jarrah, was fortuitously stopped by freeway police for speeding on the I-95, but released after a fine was paid.

As shown by the arrest of Zacharias Moussaoui, who was detained prior to 9/11, the bigger the plot, the bigger the risk of it potentially ending in failure, due to the Jihadi identity of one or more operatives being uncovered and plot secrets divulged. FBI attorneys refused permission for a search of Moussaoui's computer on libertarian legal grounds that the Patriot Act has since over-ruled. If only the computer files had been read, the US airline industry would have been alerted to the imminent threat of aircraft being used as missiles. Furthermore, it has been disclosed since 9/11, that the jailed millennium terrorist Ahmed Ressay recognized Moussaoui as having been in the Afghan camps.

Richard Reid, the shoe-bomber, who was named as an accomplice by Moussaoui, himself could have been detained before 9/11, and so might have put at risk the eventual success of the entire 9/11 mission. Richard Reid was not alone in his endeavor to bring down a plane with a shoe-bomb. In November 2001, both he and another Briton, Sajid Badat, visited Afghanistan and were given similar shoe-bombs. They returned to Britain separately in December 2001. After Reid was arrested, following the failure of his bomb attempt, some Belgian telephone cards were found on him. These were used by Badat to get in touch with Reid's terrorist contact Nizar Trabelsi, who was part of a French/Belgian Al Qaeda network.

Trabelsi, a Tunisian, was sentenced to the maximum 10 years in prison in 2003 for his designated role as the suicide bomber in another attack: one aimed at the US embassy in Paris. Such is the tangled international web of Islamist terrorist attack plans. Although terrorist cells are largely isolated, there may well be connecting network links that can be traced by security services.

A prime example is given by the 7/7 bombing of London in 2005. The cell ringleader, Mohammed Siddique Khan, was known by the British security service, MI5, to have been in communication with an Al Qaeda operative involved in another major plot involving Pakistani Muslims. But there were insufficient terrorist connections for him to have been put under surveillance: he was regarded by MI5 as a 'clean skin'. Moreover, it has recently been revealed that Mohammed Siddique Khan did have earlier links with the Anglo-Pakistani terrorists Omar Sharif and Hanif Asif, who bombed Mike's Bar in Tel Aviv in April 2003. The source of this revelation, Kursheed Fiaz, an IT company boss, was visited in Manchester by Khan and Sharif, both intent on radicalizing his employees. Sharif himself was radicalized whilst a college mathematics student.

THE CHALLENGE OF JOINING UP THE DOTS

The failure of law enforcement and intelligence services to prevent the 9/11 attacks has been described graphically as a failure to *'join up the dots'*. But had the pack of terrorist cards been stacked much higher by al-Qaeda in 2001, perhaps being twice as large, it might have all collapsed under the scrutiny of the FBI and CIA, who would then have had a much simpler task of joining the dots.

A second tragic example of dots not being joined is given by the Madrid train bombings of March 11, 2004. The cell phones used to detonate the bombs were traced back to Jamal Zougam, a Moroccan who ran a cell phone shop. Zougam was known to the Spanish authorities. He had come under Spanish police investigation, following a French tip-off that his name had been found in the address book of a French Islamist militant David Courtailler. Furthermore, a raid on Zougam's apartment revealed the phone number of Abu Dahdah, the Syrian refugee leader of the Spanish cell of Al Qaeda, who provided logistical support to the 9/11 Hamburg cell. Even so, Zougam was considered too obscure a contact to arrest. Zougam's cell phones facilitated the bombings, but he was not himself a ringleader, just a technician. Several weeks after the bombings, the Moroccan and Tunisian ringleaders blew themselves up in an apartment that the Spanish police were closing in on.

Whereas in totalitarian states, potential suspects such as Zougam might have been arrested early, interrogated and detained without legal safeguards, in democracies, the rule of law must be upheld. Individuals can only be charged if sufficient admissible evidence of criminality exists and can be presented in court. One or two circumstantial terrorist links is insufficient in itself. As more and more links are established, so the chance increases of finding incriminating evidence on a computer or in an apartment.

The identification of a sizeable community of Jihadis makes it far easier to join up the dots, because the weight of evidence increases rapidly with the size of community exposed.

ISLAMIST NETWORK ANALYSIS

In its adaptive increasingly decentralized form, the operational arm of Al Qaeda is largely divested of major hubs, the removal of which would severely impair attack capability. With technical and tactical skills learned increasingly online from Jihadi websites, much of the operational decision-making is ground-up. The loss of individual operatives is rarely a significant setback; there is no shortage of Muslim recruits ready to fill the shoes of other Jihadis. A key concept for the understanding of the close-knit social networks of Muslims is that of the *Umma*, which is the global brotherhood and sisterhood of Muslims. The small integrated world of Muslim communities is exemplified by the saying that *'The whole Umma is like one body'*. Social life for young devout Muslims revolves around mosques; Islamic bookshops and media outlets; gyms, youth clubs, colleges; as well as virtual meeting places online. Some may belong to Islamist societies such as Hizb-ut-Tahrir, which has a broad evangelistic outreach in mosques and colleges. Muslims in prison tend to group together for mutual protection, and are susceptible to radicalization influences.

Even though Islamist militants may minimize or disguise communication, such links may become manifest through clandestine surveillance of their meeting places and modes of interaction. Human intelligence, by way of tip-offs, moles, or double-agents, may provide some information on Islamist militants. Otherwise, information can be gleaned from data mining and eavesdropping, such as communication interception.

Suppose a number of operatives are actively involved in planning and preparing attacks. Any communication between two operatives, whether via a meeting, letter, phone, email, or internet, and however secret, carries a finite risk of interception by security services. Surveillance technology is increasingly sophisticated, intrusive and pervasive: Ramsi bin al-Shibh, a top Al Qaeda leader, was tracked down in Karachi after an Al-Jazeera interview, through high resolution electronic recognition of his telephone voice print by the NSA (Miles, 2005).

Within the USA, a vast amount of data mining is undertaken in the search for terrorist links. There are numerous commercial databases (e.g. World Check) that are accessed in due diligence assessments on criminal links that individuals may have. Government data mining goes far deeper. Over the past year, there has been involuntary public newspaper disclosure that the NSA taps phone calls to and from the USA, if it believes that one party is linked to Al Qaeda. Also, the NSA has also been compiling, since soon after 9/11, a massive database of telephone numbers involved in calls made within the USA. Furthermore, the US Treasury has been receiving banking data from SWIFT [Society for Worldwide Interbank Financial Telecommunication]. Such data are passed to the CIA.

These searches explore just a few of the many dimensions of the complex human transaction space within which the signal of terrorist operations may be discerned from the background noise. Other dimensions include housing, immigration, travel, transport and medical information. The full signal processing problem was designated as the technical focus for DARPA's Total Information Awareness program. This ambitious but invasive program was curtailed in 2003 over privacy concerns. Re-branded as the Terrorism Information Awareness program, TIA continues in a modified covert form. Admiral Poindexter, the instigator of TIA, likened the TIA problem to the anti-submarine warfare task of finding submarines in an ocean of noise. The detection task is easier if submarines gather in a pack. Similarly, finding terrorists is easier if the network is larger and more network connections can be identified.

From the opposing terrorist's perspective, a strategic objective is to thwart counter-terrorism attack. It is in the interests of Al Qaeda to increase the entropy of the process by which its operations are undertaken, so that these are obscured from surveillance by their dynamical complexity. One way of boosting entropy is to increase the randomness of its network connections. There is a fair degree of randomness in the way in which Islamist networks develop out of Muslim communities, and it is known that Al Qaeda looks favorably on mission candidates who depart from the traditional stereotype Jihadi image. However, some nodes are much better connected than others. Well-targeted attacks at the most connected terrorist nodes are likely to be highly disruptive. Networks with highly skewed node degree distributions are robust against the random removal of nodes, but fragile against the targeted removal of the most highly connected nodes (Calloway et al., 2000).

By comparison, random networks are especially adept at withstanding targeted attacks. This would suggest a minimal security aim of terrorists: the network should be resilient *at least* against the random detection of links between operatives. It is inevitable that a targeted counter-terrorism assault on the most connected nodes will be very damaging to network attack capability. Fortunately for diligent terrorists, special protection of such nodes makes such an assault difficult to achieve. But if it only takes the random detection of links to bring down a terrorist network, then there are just too many terrorists active at a particular time.

Even if operatives form within tight cells, links between members of different cells can form either directly, through some shared mutual human transaction, or indirectly through a virtual online transaction. For example, Al Qaeda operatives and sympathizers upload large files of Jihadi propaganda onto free file storage community sites such as www.YouTube.com and www.archive.com. A link to the file is then posted on the multitude of interconnected Al Qaeda websites, allowing others to locate and download the files. NSA tracking of Jihadi video downloads could reveal key terrorist links. It is known that Germaine Lindsay, one of the 7/7 London bombers, immersed himself in Jihadi propaganda in the week before his suicide mission. The will of another London bomber, Shehzad Tanweer, is on www.archive.com.

Intuitively, the larger the community of active operatives, the larger the number of random detected links that may arise between them, and the easier it becomes for counter-terrorism forces to join the dots, make arrests and accumulate sufficient evidence to make charges and to secure convictions. The organizational worry for terrorists is that if there is excessive planning activity for one spectacular attack, or for a wave of attacks during a short period of time, there will be a greater likelihood of more links being randomly detected, so making the security services' task of joining the dots much easier. A major part of this audacious attack planning might then be wound up in a domino-style sequence, or, in the jargon of the security services, *'like a thread unraveling a sweater'*. Terrorists will be mindful that the initial dangerous loose thread might be a raw recruit, or peripheral affiliate. It only takes one operative to be seen to be acting suspiciously to jeopardize an entire operation. Too ambitious or too many planned attacks would prove ultimately to be counter-productive, and wasteful of terrorist resources. Organizing less ambitious planned attacks would be a more resilient and patient approach, better capable of withstanding concerted counter-terrorism efforts at network disruption.

CLIQUE PERCOLATION IN TERRORIST NETWORKS

Consider attack planning from the terrorists' perspective. Suppose that there are N operatives involved at a given time. Even if the operatives are organized into mostly independent cells, extensive data mining, augmented by available human intelligence, has the potential for identifying some link between any two operatives A and Z, even in the absence of any direct intercepted communication. The fundamental Islamic concept of the Umma makes Islamist terror networks especially open to exploratory data mining, even if they may be less susceptible to insider betrayal than secular terrorist organizations. We need not fear the Islamic equivalent of the Unabomber. The cult of the shahid, or Islamic martyr, depends on popular support from the Umma, which has a key background role in Jihadi operations. Indeed, Ayman al-Zawahiri has stated (2002) that *'Al Qaeda wins over the Umma, when it chooses a target it favors'*.

Belonging to the Umma means sharing in common activities with other Muslim brothers and sisters, in preference to socializing with non-believers. Charity forms a very important part of Muslim law and tradition. There is a recognized religious duty in the Muslim world to donate a set portion of one's earnings or assets to religious or charitable purposes, and additionally, to support charitable works through voluntary deeds or contributions. However, anomalous financial transactions may link operatives A and Z to illegal terrorist funding.

In respect of shared activities, operatives A and Z may have attended the same radical mosque; or studied in the same college or madrassah; be members of the same Islamic society or youth group; be recent converts to Islam; have participated in the same Islamic conference; surfed the same Jihadi website or downloaded the same propaganda video; be veterans of the same Jihadi campaign (e.g. Bosnia or Iraq); trained in the same military camp; have been involved in crime to finance political militancy; have been in the same prison; or have visited the same foreign Muslim country at the same time.

Even if there is only a 1% chance of a specific factor linking A and Z, given that there are at least ten alternative factors (financial, social, communicational etc.), there could be an approximate 10% chance of some linkage. As a concrete illustration, for a group of five Jihadi suspects, counter-terrorism investigations might be expected to reveal a link of some kind between one pair of them. The high interdiction rate (80% to 90%) for planned Jihadi attacks in USA and Europe would suggest reasonable success at spotting links.

The chance of a link being revealed may not correlate closely with the strength of the link within the terrorist organization. The connectedness structure of the virtual network of online Jihadi communication is very different from that of a physical network. Al Qaeda has generated a family of interconnected websites, which has built-in redundancy and survivability. This virtual cyber space structure has the effect of randomizing link detection. Furthermore, it may be easier to detain and get information about a person more at the periphery of a terrorist organization, than from someone at a hub, who has extra identity protection and is more security-conscious. Even a marginal operative may have, on his computer, Jihadi files which would implicate others.

The challenge facing the counter-terrorism forces is to make some sense out of a tangled web of links between possible Jihadi suspects. In order to be able to join up the dots, counter-terrorism analysts need to be able to recognize the pattern of a Jihadi community. It turns out that the number of operatives N involved in planning attacks has a tipping point in respect of the ease with which the dots might be joined by counter-terrorism forces. The opportunity to spot a community of terrorists increases nonlinearly with N : above a critical number, the opportunity improves rapidly. Casting a net to haul in terrorists becomes much easier if they come along in a shoal, rather than a few at a time.

This nonlinearity has been discovered and modeled mathematically through analytical studies of random Erdos-Renyi (ER) networks, conducted by a group of Hungarian biophysicists (Derenyi et al., 2005). They introduce the notion of k -clique percolation through the following basic definitions: (1) A k -clique is a complete subgraph of k nodes. (2) Two k -cliques are adjacent if they share $k-1$ nodes. (3) The union of a sequence of adjacent k -cliques is called a k -clique chain. (4) Two k -cliques are said to be k -clique-connected if they are parts of a k -clique chain. (5) A k -clique percolation cluster is a maximal k -clique-connected subgraph.

For a graph with N nodes, Derenyi et al. show that a percolation transition of k -cliques occurs when the probability of two nodes being connected reaches the critical threshold: $p(k) = [(k-1)N]^{-1/(k-1)}$. For $k=2$, this yields the classic percolation transition threshold result of $1/N$, because 2-clique connectedness is just regular connectedness. This is not so helpful in the counter-terrorism context, since a 2-clique is merely a single link, which does not reveal very much, and is not in itself incriminating within a western justice system: as with Jamal Zougam, it is not a crime to know a terrorist, or to be known by one.

However, the case where $k=3$ is useful, because a 3-clique is a complete subgraph of 3 nodes, and is a building block of a realistic community. For $k=3$, the percolation transition occurs when the probability of two nodes being connected reaches the square-root of $1/(2N)$. For $N=50$, this transition is at 10%; for higher values of N , the transition probability is correspondingly lower.

The significance of this analysis for a terrorist mastermind is as follows. Network operations should be resilient against a certain degree of disruptive counter-terrorism action. Allowing for a randomized 10% chance of some linkage between two Jihadi suspects, then the number of operatives actively involved in attack planning should be kept limited to about fifty. Below this tipping point, the pattern of terrorist links may not necessarily betray much of a signature to the counter-terrorism services. However, above the tipping point, a far more obvious signature may suddenly become apparent in the guise of a large connected network cluster of dots, which might give away the presence of an active Jihadi community. Computer simulation shows how the whole network might be quite readily wound up. Apart from controlling the length of pipeline of planned attacks, this limit of fifty serves as a constraint on the multiplicity of synchronous swarm attacks, and on the scale of the most ambitious, technically sophisticated, and labor-intensive terrorist operations, such as involving the development of weapons of mass destruction.

A SMALL TERRORIST WORLD

It is a small world, as much as for terrorists as for everyone else. A human chain of six links should be about sufficient to connect anyone on the planet to anybody else. The intelligence services required a chain of just three links to get to Abu Musab al-Zarqawi. First, Jordanian intelligence officers captured one of Zarqawi's junior operatives, Ziad Khalaf al-Zerbouly, who was working as a customs official, helping in smuggling money and materiel. Although ignorant of Zarqawi's whereabouts, under interrogation, Kerbouly revealed the name of Zarqawi's new spiritual advisor: Sheikh Abdel Rahman. A US special forces team located Rahman, placed him under surveillance, and tailed him to a house near Baqubah, where he had his fatal meeting with Zarqawi. As in the man-hunt for Zarqawi, the interrogation, or surveillance, of any known network operative, even a lowly foot-soldier, can be instrumental in providing sequential leads for tracking down senior leaders in the terrorist hierarchy.

Human beings are social creatures, and have contact with each other through social networks. Terrorists are no exception. Islamist militants, in particular, live within close-knit Muslim communities, on which they depend for moral support and reinforcement of their ideology. Jihadis are discouraged from mixing with unbelievers. One of the most influential and uncompromising of radical imams in Britain, Abu Hamza, has urged: *'Don't sit with people who are mocking the signs of Allah'*. Islamist militant groups who heed this injunction may well be much more vulnerable to the external data mining of their confined transaction space than to being compromised by internal betrayal or infiltration by counter-terrorism agents.

There is a trade-off between the external and internal risks to a terrorist organization. The more social interaction there is with outsiders, the more opaque and uninformative is the outcome of any attempt at data mining, but the risk is higher of infiltration by a secret agent posing as a Jihadi. By contrast, the less social interaction there is with outsiders, the less vulnerable a group is to infiltration, but the risk of disruption through community data mining is greater. Islamist militants are success-oriented, and will be concerned over the intelligence trails left by an excessive number of operatives, and the potential disruptive effect of counter-terrorism network surveillance. This anxiety promotes caution, and a restriction of the scale of attacks, and the multiplicity of synchronous attacks, that can be prudently planned within the same theater of operation, during a particular time interval.

Five years have elapsed since 9/11. Since then, the interdiction rate of planned macro-terror attacks on the US and Western Europe has been consistent with that achieved by counter-terrorism forces in other major terrorist campaigns against leading military powers, e.g. the IRA in the UK. Furthermore, the annual rate of attack planning has been running at a few attempts per country. The resultant outcome has been a few sporadic successful Jihadi attacks, e.g. Madrid (March 11, 2004) and London (July 7, 2005). This experience can be elucidated using network analysis concepts.

Counter-terrorism action has the deterrent effect of imposing a fundamental constraint on the planning of a wave of major terrorist attacks. Terrorists ignore this constraint at the risk of suffering large-scale network disruption. There is a tipping point in the number of active terrorists who can be involved regionally in attack planning. Beyond the involvement of about 50 active terrorists, it becomes much easier for counter-terrorism forces to join up the dots and identify an active terrorist community well enough to make arrests, and gather sufficient evidence to secure convictions. When only a handful of active terrorists are involved at a given time, the strength of courtroom evidence is likely to be significantly weaker, and far more people are likely to be arrested than charged or convicted. Indeed, since 9/11, more than seven hundred people have been arrested in Britain under the Terrorism Act, but half have been released without charge and only a score convicted.

Since 9/11, all the most spectacular plots have been interdicted in Britain, the rest of Europe, and around the world. Consider the foiled Jemaah Islamiyah (JI) plot to explode six large truck bombs around Singapore shortly after 9/11. Outside the Middle East, this is the most audacious and ambitious terrorist plot conceived after 9/11. Had it succeeded, the death toll might have exceeded that on 9/11. This plot involved three JI cells in laying the groundwork for the attacks. In this case, a tip from the public drew attention to a Singaporean of Pakistani origin, who boasted in a bar of having met Osama bin Laden. The security services started to monitor his close associates, one of whom was seeking to buy a large amount of ammonium nitrate; another had family links with Islamist extremism. Gradually the whole plot unraveled with many arrests.

Close to the 5th anniversary of 9/11, on August 10, 2006, there was public disclosure of a brazen Jihadi Bojinka-like plot to use liquid explosives to bomb ten planes flying across the Atlantic from UK to USA. Involving ten teams of two suicide bombers, this swarm attack proved to be excessively ambitious. In the aftermath of the 7/7 London bombings, a tip from a member of the British Muslim community about suspicious behavior by an acquaintance alerted authorities to the alleged conspiracy, and a neighbor of the alleged plotters helped confirm those suspicions. Counter-terrorism officials then used telephone records, emails and bank records to connect the suspects and build a detailed picture of the conspiracy. In line with Terrorism Information Awareness procedures, spending habits and bank accounts also were data-mined.

Large complex plots involving many terrorists are highly vulnerable to being unraveled through diligent counter-terrorism surveillance. In the game of checkers, having many pieces on the board carries the risk that a sizeable connected group might be swept away in a single adversarial move. Similarly, in the asymmetric war game of terrorism, having too many active terrorist operatives in the same field induces a degree of congestion in the space of terrorist operations, and carries a heightened risk of 'dots being joined' by security services.

REFERENCES

- Al-Zawahiri Ayman *Knights under the Prophet's Banner*, London, 2002.
- Abu Hamza al-Masri *Allah's Governance on Earth*, Deluxe Printers, London, 2001.
- Barabasi A-L. *Linked* Penguin, London, 2003.
- Bell S., *The Martyr's Oath*, John Wiley & Sons, 2005.
- Calloway D.C., Newman M.E.J., Strogatz S.H., Watts D.J. "Network robustness and fragility: percolation on random graphs." *Phys. Rev. Lett.*, Vol.85, No.25, 5468-5471.
- Cohen R., Havlin S., Ben-Avraham D. "Structural properties of scale-free networks", Wiley-Vch Verlag, Berlin, 2002.
- Derenyi I., Palla G., Vicsek T. "Clique percolation in random networks," *Phys. Rev. Lett.*, 94, 2005.
- Farley J.D. "Breaking Al Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making)," *Studies in Conflict and Terrorism* **26** (2003), 399-411.

Gunther G., and B. L. Hartnell, "On Minimizing the Effects of Betrayals in a Resistance Movement," *Proceedings of the Eighth Manitoba Conference on Numerical Mathematics and Computing (September 28-30, 1978)*, 285-306.

Jacquard R. *In the Name of Osama bin Laden*, Duke University Press, 2002.

Lawrence B. *Messages to the world: the statements of Osama bin Laden*, Verso, London 2005.

Miles H., *Al-Jazeera*, Abacus books, 2005.

Newman M., Barabasi A-L, Watts D.J. *The structure and dynamics of networks*, Princeton University Press, 2006.