Routledge
Taylor & Francis Group

Journal of Policing, Intelligence and Counter Terrorism

ISSN: 1833-5330 (Print) 2159-5364 (Online) Journal homepage: http://www.tandfonline.com/loi/rpic20

Intelligence for Counter-Terrorism: Technology and Methods

Abraham Wagner

To cite this article: Abraham Wagner (2007) Intelligence for Counter-Terrorism: Technology and Methods, Journal of Policing, Intelligence and Counter Terrorism, 2:2, 48-61, DOI: 10.1080/18335300.2007.9686897

To link to this article: http://dx.doi.org/10.1080/18335300.2007.9686897

Intelligence for Counter-Terrorism: Technology and Methods

ABRAHAM WAGNER
School of International and Public Affairs,
Columbia University

ABSTRACT

In recent years, access to new information, communications and weapons technologies has enabled criminal and terrorist operations on a scale previously unobtainable. While the number of terrorists and terrorist organizations has increased, the nature of their operations has changed dramatically as well. Understanding and countering modern terrorist operations poses a significant challenge for law enforcement and security services. In many cases technologies open to terrorist abuse have evolved far more rapidly than the technologies and methods needed to counter them effectively, even in the most advanced nations, which are at least a generation behind the terrorists in some areas. In countering terrorism, police and intelligence services need timely and effective access to terrorist communications, as well as the ability to interdict weapons shipments and other logistics.

Given the nature of the new technologies, these have become very difficult tasks. As terrorists have become increasingly sophisticated in their operations, demands on counter-terrorist operations and technologies have escalated as well. In meeting these challenges it is important to note that in some cases the solution will involve both new laws as well as new technologies. In other cases, it may be necessary to face the facts that some operations are currently beyond the reach of the law or the technology base, and alternative approaches will need to be found. This article reviews the current technology base used by terrorists; explores the challenges posed for counter-terrorist operations; and suggests areas where new technologies may be of use in meeting these challenges.

Introduction: The intelligence challenge of counter-terrorism

There is little question that recent years have seen an increase in terrorist activities worldwide, including new organizations and a far larger number of terrorists and attacks. The Middle East, Europe, Asia and North America have all seen increasing numbers of terrorist attacks. Thus, governments in these regions require intelligence operations that are responsive to this growing threat. Failures of the United States law enforcement and intelligence services with regard to the 9/11 attacks in 2001, as well as terrorist incidents in Europe and elsewhere that were not detected by the various intelligence services clearly demonstrate the nature of this challenge (National Commission Report, 2004; Report of the Joint Inquiry, 2002). While it is not reasonable to expect that even the best intelligence services will detect every possible attack, it is certainly the case that a better job can be done with respect to the evolving terrorist threat.

At the same time it is also the case that many intelligence services have failed to adapt to the requirements of the post Cold War era. Many of the expensive collection systems in use were designed to collect intelligence against the Soviet Union and specific Cold War requirement, while analytical and other tools were also focused on Cold War needs. In the United States, for example, large numbers of linguists were trained in Russian and other languages of the former Soviet Union and its satellites, while few were trained in Arabic and other Middle Eastern languages, or were familiar with the culture and other regional issues important to effective intelligence against terrorist targets.

An additional problem, particularly important in the United States, was a failure to integrate domestic police intelligence with security intelligence so that data could effectively be disseminated or shared among the various organizations responsible for counter-terrorist operations. This was a major problem identified in the 9/11 studies, and an attempt made to address this in the 2004 Intelligence Reform Act (National Commission Report, 2004; Report of the Joint Inquiry, 2002; Report of the Commission on Intelligence Capabilities, 2005).

New technologies and resources available to terrorists have clearly made the intelligence problem much more difficult. Modern communications technologies, such as cell telephones and the Internet, in particular, have enabled terrorist operations on a new scale. Use of containerized shipping and the explosion in worldwide commerce have also enabled terrorists to move weapons and other materials with considerable ease. Increasing use of such technologies by terrorists, with corresponding improvements in operational security, have made timely

and accurate access to critical data by intelligence agencies more difficult. For their part, many terrorists have changed their mode of operations, adopting these new technologies and implementing various operational security measures designed to avoid or defeat sophisticated intelligence collection operations.

Strategic intelligence on terrorist organizations and infrastructure

At the strategic level the requirements for intelligence for counter-terrorism are similar to other areas in terms of a fundamental need for realistic threat assessment that evaluates the nature and evolution of both foreign and domestic threats. Unfortunately, much of what has been done in this area over the past several years is confused with inaccurate speculation and hyperbole, as the 9/11 Commission described in considerable detail (National Commission Report, 2004). In terms of terrorist organizations such as Al Qaeda and others there is an ongoing need to track the evolution of these groups as well as their operational capabilities and infrastructure. Indeed, there is ample evidence to suggest that Al Qaeda has moved from a hierarchical model, directly sponsoring and managing various operations to a 'franchise' model where it indirectly supports and encourages domestic groups.

An increasingly serious set of threats, then, comes from the domestic Islamic populations in various nations, which are subject to being radicalized and capable of providing the manpower and other resources for specific terrorist operations. Attacks in Madrid, London and elsewhere clearly demonstrate the seriousness of such threats. Here, strategic intelligence analysts need to understand the domestic groups as well as the organization of terrorist cells, their leadership and infrastructure. At the same time, there is a need to also understand the interactions between these domestic groups and foreign organizations such as Al Qaeda that support them.

Accomplishing this task is not a simple or magical process. Nor is it one that can be accomplished overnight. It is one that requires the responsible intelligence services to undertake a serious, sustained effort over time. Resources need to be made available for the collection, analysis and fusion of data over time. Intelligence is not like a water faucet – you cannot simply turn it on when you need it. Nor is it possible in most cases to make up for lost time by simply 'pouring cash' on to an intelligence problem. There is no real alternative for systematic investment in sustained effort over time. A major element of this investment needs to be in the relevant language and analytic skills. The vast amount of open source material, as well as other secret materials collected, is in a variety of local languages that require these skills. The

shortage of qualified and cleared linguists in even the more common languages, such as Arabic and Farsi is staggering. At the same time, the number of schools and other language training programs for these critical dialects are seriously limited (Report of the Commission on Intelligence Capabilities, 2005).

Strategic intelligence collection

Unlike the Cold War problem, where the Western powers were dealing with a 'denied area' and very limited data, the problems in the counter-terrorism area are quite the opposite, where massive amounts of data are available to support strategic intelligence analysis. The vast majority of relevant information is 'open source' data and freely available from Internet web sites, broadcast media, publications, and elsewhere. The number of radical Islamic web sites, for example, is large and growing rapidly (Weimann, 2006).

Al Qaeda and its ideological affiliates publish and broadcast extensively. In many cases these are organizations with a literalist ideology derived from eighth century Islamic tradition utilizing the best 21st century technology to support their cause. Indeed, modern terrorists are utilizing all of the modern media to support various aspects of their operations, such as propaganda, recruitment, fundraising, and actual operations (Cordesman & Wagner, 2005; Wagner, 2005). Certainly the advent of the Internet, as well as satellite-based television channels and other media, where the marginal costs are close to zero, have been a great boon to all media users, and terrorist organizations have taken full advantage of these realities.

Supplementing the massive amount of open source information with more traditional, non-public sources of intelligence is far more difficult. Communications intercepts (COMINT) against terrorist operations is both difficult, and falls more into the realm of operational intelligence, covered in greater detail below. Similarly, human source information, obtained either from penetration of terrorist organizations with intelligence operatives, or recruitment of cell members and related parties is an operational matter of greater relevance to the concerns covered below.

TECHNOLOGY CHALLENGES

The most significant technology challenges in the area of strategic intelligence come in the processing and analysis of the massive amount of data available, rather than in its collection. The problems are really ones of 'too much data' rather than 'too little'. The data are mostly in Arabic and languages other than English, and a significant amount are broadcast media, and not digital record copy. Even five years past the 9/11 "wake

up call" the intelligence services of the United States and other nations are still woefully deficient in language and related processing capabilities needed to meet this challenge (Wagner, 2007a, Wagner, 2007b).

In terms of available linguists in Arabic, for example, the United States has failed miserably. There are relatively few skilled and cleared linguists working now, and the language programs needed to produce new linguists are very limited at best – both Government-sponsored as well as academic programs utilized by the Government and students seeking Arabic training, who aspire to work for the Government.

It has been clear for decades that this problem cannot be solved with manpower alone, even if more training programs could be established. Monitoring operations during the 1979 Iranian Revolution, Soviet Military operations in Afghanistan and others illustrate that the sheer volume of foreign language material quickly outstrips all available linguistic and related analytical resources. Clearly the costs are prohibitive. What is needed is a set of enabling technologies that can support the linguists and analysts that are available to make best use of these scarce resources. Where the data are in digital form, such as on Internet web sites or from digital telephone systems, new search engines and related systems are a critical tool for this requirement. Increasingly, such engines incorporate advanced features utilizing artificial intelligence to locate materials of relevance. At the same time, the revolutionary increases in processing power, memory and other aspects of modern computing enable such automated analyses on a cost-effective basis (Wagner, 2005; Wagner, 2006b: Wagner, 2007a).

For the mass of data that cannot be searched in this manner the technology problem is far greater. Automated systems to convert speech to digital text and perform related translation and search functions are still in their infancy (Wagner, 2007a, Wagner, 2007b). For decades, research and development programs within the Intelligence and law-enforcement communities have been under-funded and not received adequate priority. Early programs in the United States, were funded by the Defense Advance Research Projects Agency (DARPA), and not by the Intelligence Community.

The current situation should be viewed as one case of 'intelligence failure' and a national embarrassment; it is a case of misplaced priorities and management failure on the part of the intelligence community. Some of the billions of dollars spent on exotic collection platforms might be more usefully employed on a 'Manhattan Project' for automated translation and processing. Filling up the 'vacuum cleaner' with data that cannot be used is a pointless exercise.

Operational intelligence on specific operations, individuals and related activities

OPERATIONAL INTELLIGENCE REQUIREMENTS

It is hard to overstate the need for operational intelligence with respect to specific terrorist organizations, their capabilities, and plans for future attacks. Continuing attacks by Al Qaeda clearly demonstrate the magnitude of the ongoing problem. Specifically, this breaks down into actionable intelligence in areas such as:

- data related to specific terrorist cells and capabilities, including information on groups and individuals, weapons and other supplies, as well as locations and infrastructure
- information on planned attacks, such as location(s), time, personnel and specific attack plans

While such intelligence is highly desirable, it is also the case that it is unlikely ever to be complete and accurate in most of the cases. The intelligence business is most often one of working with partial and faulty data. Some intelligence is simply wrong, even if it comes from highly secret sources; some plans never actually materialize and, there are many cases of 'false alarms'. One good example of this problem came shortly after the 9/11 attacks, when the United States had a supposedly reliable intelligence source known as 'DRAGONFLY', who told of a terrorist nuclear device in New York City. Fortunately, this turned out to be a case of faulty intelligence and there was no such device (Wagner, 2007a).

State security and other services simply cannot respond to everything, as this would quickly exhaust the personnel and resources available. Thus, the problem is complicated by the need to identify what intelligence data are most credible and serious, and then, which alarms require a response.

OPERATIONAL INTELLIGENCE COLLECTION

During the Cold War, the United States and allied nations moved very heavily into the use of 'technical' collection systems to meet the requirements of the time and difficulties involved in using human sources against the 'denied areas' of the Soviet Union and allied Warsaw Pact states. At the time these collection systems provided access to adversary communications systems that were largely unsecured, as well as images of military facilities that were not hidden from satellite photography. Such technical collection operations were highly cost-effective and successful with respect to the intelligence requirements of the Cold War era (Wagner, 2007a).

Today, however, the requirements for counter-terrorist intelligence and the lack of technical access to terrorist communications has caused most intelligence services to view human sources (HUMINT) as some sort of magical solution to the collection problems of the current era. Advanced digital communications systems, such as cellular telephones and the Internet, have become as widespread and pervasive, and are nowhere near as technically accessible, as the antiquated Soviet systems of the Cold War era. Even where technical access to various systems is possible, individual phones are most often used by 'anonymous' cash subscribers and supporting data about numbers and their users do not exist. Comments about the 'HUMINT solution' often come from journalists and others with little understanding of the human intelligence business, and the actual difficulties in such operations.

Certainly HUMINT is an essential element of the operational intelligence process, and where possible can yield critical information about terrorists and their operations. In many cases, however, this is far easier said than done. Most terrorist cells are highly compartmentalized, and often composed of close friends and family members. Penetration by any outsider may be near to impossible. The most productive path may be to try and recruit sources either in or near a terrorist cell with money. Here, too, the results may lead to false or misleading intelligence, but this is the nature of the HUMINT business. When it works, it can yield important results, but it is not the sort of thing that can be relied upon for timely and accurate warning. At best, HUMINT is only one type of intelligence source that needs to be integrated with other available sources and subjected to expert analysis.

ACCESS TO TERRORIST COMMUNICATIONS

Over the last several decades, communications intercept has increasingly become the cornerstone intelligence capability, and for a good reason. Communications technologies have evolved by orders-of-magnitude, and decreased in cost, so that they have come into widespread use in virtually every nation. Business people, school children, and terrorists alike all take full advantage of what modern telecommunications offer. Cellular telephones, the Internet, and other modern systems have proliferated around the globe at rates never imagined a few short years ago. For the terrorist they offer the ability to communicate and execute worldwide operations with reasonable expectations of privacy and security. It is hard to underestimate the utility of communications intelligence or COMINT in the modern era. While advanced COMINT collection systems provided a critical 'window' into adversary operations, most intelligence services became spoiled by what was easy access to these important communications (Wagner, 2007a; Wagner 2007b).

As cell phones and the Internet have become 'tools of the trade' for terrorists, access to these communications has become an increasingly

difficult and costly problem for several reasons. Where terrorists exercise good operational security (OPSEC), changing SIM cards and phones frequently, with no information as to the actual ownership of any cell number, finding a particular individual presents substantial problems. Similarly, careful use of Internet accounts, servers and access points makes locating terrorist e-mail problematical as well. In many cases where terrorist communications have been found, it is because the terrorists have been either stupid or sloppy in their operations – or both, exercising poor OPSEC. In the future, intelligence operations cannot depend on this poor behaviour. There is most likely a learning curve here, and the terrorists will learn.

It is important to bear in mind that this is not a binary issue – access or no access. Technical access is becoming more difficult and, hence, more costly and will continue to do so as more modern systems come into use and communications volumes increase. At a minimum, the 'golden days of COMINT' are over. Intelligence analysts will need to live with limited access, using analytic tools to make better use of the partial and incomplete data that are available, integrating them with both HUMINT and open-source reporting.

THE SEA OF DIGITAL DATA

To better appreciate the technical collection problem, it is worth noting that nothing short of a major technical revolution has taken place over the past decade, with the world becoming a truly digital one. Communications have increasingly merged with computing, while virtually all other media – entertainment, music, movies, and education have all moved into digital form. Whatever 'it' is, it is now digital. The result has been an explosion in the volume of digital data, not only stored, but being transferred and 'downloaded' on all sorts of devices.

The net result of this digital explosion is what can be termed a 'sea of digital data' that has flooded computing and communications systems. Order-of-magnitude increases in both storage and communications bandwidth have made this both practical and increasingly cheap for users. Indeed, the marginal cost of communications is rapidly approaching nought. For intelligence services, facing this sea of digital data, the collection, storage and even sorting become daunting and costly tasks. Clearly most of the 'data' in this sea are of no intelligence value, so the challenge becomes one of focusing collection and sorting efforts to areas, where they can be most productive. The intelligence challenge shifts from one of 'is access possible?' to 'what resources are needed to locate useful data in the mass of data that can be accessed?'.

Here, the development of sorting and analytical tools by the US intelligence community has been far behind the requirement. Over the years, major investments, amounting to many billons of dollars, have

been made in advanced technical collection programs such as ground stations, satellites, aircraft, ships and other technologies. As indicated above, these collection programs were highly successful against the targets of the time, such as the Soviet Union and Warsaw Pact states, which employed relatively antiquated communications systems. At the same time, less attention was paid to how collected data could effectively be sorted, translated and analyzed. As indicated above, machine translation has been inadequately supported for many years and related tools have not been developed as well. In the past few years, investments have been made in what has been termed 'data mining' – an area that should show great promise (Wagner, 2005).

FINANCIAL TRANSFERS

Closely related to terrorist communications are efforts to track funds used by terrorists and related organizations (Ehrenfeld, 2003). To some extent, this parallels intelligence efforts to identify money laundering related to illegal drugs and other criminal activities and can usefully build on the experience and systems already developed.

A word of caution is in order here, however. It is wrong to assume that terrorists are the same as either drug lords or corrupt leaders. First, most terrorist operations do not require large sums of money, and are not seeking to live a life of luxury with hidden funds. Estimates reported by the US 9/11 Commission placed the total cost of the 9/11 operation to Al Qaeda at about $300,000, of which some was left over and sent back for future Al Qaeda operations.

Other attacks have been in this general range and most have cost far less. None thus far has been a multi-million dollar operation requiring complex fund transfers. Further, terrorists seek death – not profits. For terrorists money is only a means to their goals and not an end in itself.

The 'good news' is that terrorist operations require funding, and it is often possible to trace funds in intelligence and law enforcement. The 'bad news' is that these operations require relatively little money, compared to military operations. The actual sums involved are not huge. Researchers such as Rachel Ehrenfeld and others have shown that these are indeed low cost operations. Reports of the US military from Iraq, as well as the Israeli military and security services all make a point of just how cheap and poorly-made suicide bombs are (Ehrenfeld, 2003).

Even the supporting infrastructure, which in most cases consists of small, clandestine workshops set up in garages, apartments and small industrial spaces are not costly enterprises, and virtually none are anything approaching a modern industrial facility. In Iraq for example, even the most deadly improvised explosive devices (IEDs) are low cost, utilizing explosives, spare parts and commercial vehicles. As a practical

matter, moving the sums which terrorists do require around the globe can be accomplished in a number of ways, and can be done in ways that are likely to avoid detection, where decent operational security is maintained. For smaller sums, cash can be sent using commercial express services such as FEDEX or DHL, thus avoiding wire or bank transfers and the high technology intelligence centres monitoring such transfers. Some terrorists have already been identified as using precious gems and metals as another means to move funds and finance operations (Wagner, 2006a). On balance, sophisticated collection operations and monitoring are probably more applicable to drug money laundering and other criminal activities, but applying these resources to counter-terrorism is certainly an added value to investing in these capabilities.

Of greatest importance in this area are two things. First, at an operational level, it is highly significant if funding can be tied to a specific organization, operation or individual. Second, it is also important to tie terrorist funding to specific sources, such as Iranian or Saudi sponsors, or various Islamic 'charities' that function as terrorist sponsors, so that political and other pressures can be brought on these state sponsors and related activities to cease such support. In the case of both foreign state support and the established charities much more can be done to identify and stop this support. Within the United States several such Islamic charities have enjoyed federal tax exemption and continue to operate openly, even after their leaders have been convicted and jailed on terrorism charges. As for state sponsors, the United States continues to focus attention on Syria, while the vast sponsorship of funding from Saudi Arabian sources is largely ignored. Non-governmental terrorist researchers have provided substantial data already and significant work remains to be done by the responsible security services (Ehrenfeld, 2003).

IMMIGRATION AND BORDER CONTROL

If nothing else, the 9/11 attacks on the United States were a 'wake up call' that the nation faced serious border control problems (National Commission Report, 2004; Report of the Joint Inquiry, 2002). The 19 Al Qaeda operatives who entered the United States came through John F. Kennedy and Newark airports with passports and valid visas, causing the United States to radically tighten visa and inspection procedures post-9/11. Unfortunately, this gave rise to implicit assumptions that all future foreign terrorists would attempt to (a) enter the United States through an airport or legitimate border control checkpoint; and, (b) would not attempt to enter the United States with a European Union passport and no visa, under the established I-94 visa waiver program (Wagner, 2007a; Wagner, 2007b). By a recent INTERPOL estimate, there are currently some 25,000 EU passports that have been reported 'lost' or 'stolen' and for reasons that almost defy imagination, do not appear in a data base at any United States port of entry. No similar data are available for the

United States, but the number of US passports in the wrong hands must be substantial. Various US officials have stated that US passports that have been reported as lost or stolen will be detected at a point of entry with the requisite computer equipment.

Some five years following 9/11, the United States still has Southern and Northern borders that are largely open and uncontrolled. A major national debate has evolved over the fact that some 11-14 million people have illegally entered the nation in recent years, and an estimated 6,000 illegal aliens stream into the United States daily. To think that no terrorist could enter the United States from Mexico or Canada along with the flood of illegal aliens is complete nonsense, but as yet no policy or program has been developed to meet this obvious challenge.

What the United States has done as a 'solution' is to make the visa process for non-European visitors more difficult and annoying. It is not likely that this change has stopped any dedicated terrorist from entering the United States, but it is certain that it has caused major problems for United States commerce, families, and legitimate tourists. This has been a pretense of addressing the problem seriously, while it has diverted attention and resources from the real issues. At the same time, the United States and other nations have begun collecting data from those entering the nation, such as digital photos and single fingerprints, while it is not yet clear that these data are useful in any serious counter-terrorism program.

Not every Moslem traveler is a terrorist, and there is a need to effectively sort potential terrorists from others. Arresting and harassing the innocent does not win friends. Cooperation of domestic Islamic groups and individuals is essential to an effective HUMINT effort, and it is clear that insults and harassment serve to impede serious efforts to work with this community on intelligence operations (Wagner, 2007a).

THE LOGISTICS NIGHTMARE

One aspect of the border control problem of particular concern is raised by the massive level of imports, and the distinct possibility that weapons, explosives and other materials useful to terrorists can be brought into the country without detection. Taking one example, some 30% of all goods coming into the United States enter through the ports of Los Angeles. With current technology it is simply impossible to search all incoming cargo containers (Flynn, 2004; Lipton, 2005; Report of the Inspector General, 2005). Indeed, less than 10% of the container flow is inspected by any means now, and an even smaller percentage is inspected 'thoroughly'. It is a fact of current commercial life that any attempt to inspect 100% of the flow would simply kill the economy. For terrorists and drug dealers alike the corresponding reality is that they are not shipping gold or some highly precious cargo. If inspections get better,

they can simply ship more and factor the 'loss' into their operations. The situation has become particularly bad on the United States' Southern Border, where armed Mexican Army trucks have been found bringing illicit drug shipments into the United States.

It would be desirable that some advanced inspection technologies will help over time, even deterring some terrorist operations. Most important in this area is the detection of radioactive materials being shipped into the country for terrorist uses. Here there is at least some promise that various detection technologies currently under development, or being tested, (now outside the United States) may prove useful. Again the United States has failed to cover itself with glory in this regard. The approach of the responsible Department of Homeland Security has been characterized as very little and very late by that agency's own Inspector General (Report of the Inspector General, 2005). Poor management and internal disputes have resulted in projects that are inadequate and late.

Such advanced inspection technologies, along with a program of tagging and tracking containers may prove useful in imposing some level of control on the situation, which does not presently exist. In the end, it may be the case that there are some problems that are just too hard, and good technical solutions may not exist. It is likely that airplane hijacking with weapons and explosives can be stopped, but import of weapons and explosives into the country cannot – at least not absolutely. Cargo containers are, at best, a long-term problem and it is important to look for other weak points in terrorist operations (National Research Council, 2002).

Conclusion: When the dots are connected

The great criticism of the intelligence failures related to the 9/11 terrorist attacks, as well as others, has been one of failing to 'connect the dots' and drawing the correct conclusions from data that were available, or should have been detected. While such criticism is certainly justified, it is also important to note the numerous examples of failure to act when good intelligence was available and the dots were connected. Here it is possible to consider four historic cases:

- German invasion of the USSR (Operation 'Barbarossa', 1941)
- Japanese attack on Pearl Harbor (1941)
- Egyptian, Syrian and Jordanian attack on Israel (October War, 1973)
- Soviet invasion of Afghanistan (1979)

Looking at these cases there are three reasons why there was a failure to act even when the dots were connected:

- Leadership failures – through either disbelief or shock when national leaders were presented with accurate intelligence (such as 'Barbarossa' and the October War)
- Security – measures to protect intelligence sources and methods that prevented effective utilization of the available intelligence
- Dissemination from the 'top' to the proper action officers delayed too long for an effective response

In each case, the net result was a disaster, and raises the question as to whether the result could have been better. For each of these cases, studies of the problem have given a very definite 'yes'. Better leadership mechanisms and organizations have been implemented in all of the nations covered by these examples, but the question remains as to whether this outcome can really be stated with confidence. Virtually no single nation has a single point of failure any more. Looking at the second of the two issues discussed, most modern nations have improved their security and dissemination systems so that vital intelligence is flowing effectively to those who need it. Certainly, there is a great deal more to be accomplished, but in most cases the situation has greatly improved.

According to some analyses, the current wave of worldwide terrorism has another two decades to run before it subsides. Over this period, terrorists will continue to refine their techniques and operations, employing new systems, as they become available and improving their operational practices for those in use. This poses a serious and ongoing challenge to the intelligence services of those nations combating terrorism. Meeting this challenge requires an ongoing commitment and investment of resources by the intelligence services involved. For too long, intelligence services have failed to meet this challenge effectively. There is an indispensable need for further investment in, and substantial improvement of, the intelligence services tasked with counter-terrorism.

REFERENCES

Cordesman, A.H., & Wagner, A.R. (2005). *The lessons of modern war*. Volume V: The war in Iraq. New York, NY: Harper-Collins.

Ehrenfeld, R. (2003). *Funding evil: How terrorism is financed – and how to stop it*. New York, NY: Bonus Books.

Flynn, S.E. (2004). *America the vulnerable: How our government is failing to protect us from terrorism*. New York, NY: Harper-Collins.

Lipton, E. (2005, May 8). U.S. to spend billions more to alter security systems. *New York Times*, p. 1.

National Commission on Terrorist Attacks Upon the United States (9-11 Commission) (2004). *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States.* New York: W. W. Norton & Company.

National Research Council. (2002). *Making the nation safer: The role of science and technology in countering terrorism*. Washington, DC: National Academies Press.

Report of the Commission on the Intelligence Capabilities of the United States regarding weapons of mass destruction: Report to the President of the United States. (2005). Washington, DC: Executive Office of the President.

Report of the Inspector General. (2005). Washington, DC: U.S. Department of Homeland Security.

Report of the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence in Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001. (2002). Washington, DC: United States Senate.

Wagner, A R. (2005). Terrorism and the internet: Uses and abuses. In M. Kandel & A. Last (Eds.), *Cyberterrorism* (p. 1-28). New York, NY: World Scientific.

Wagner, A R. (2006a). Information operations and international law. In K. von Knop, H. Neisser, A. Salnikov & B. Ganor (Eds.), *Security, terrorism and privacy in information society,* (pp. 373-398). Berlin: Bielefeld, W. Bartelsmann Verlag, GmbH & Co.

Wagner, A R. (2006b). Terrorist use of new technologies. In P. Katona, M. Intriligator & J. Sullivan (Eds.), *Countering terrorism and WMD*, (pp. 122-147). London: Routledge.

Wagner, A R. (2007a). *Meeting the terrorist challenge: Coping with failures of leadership and intelligence*. New York, NY: Harper-Collins.

Wagner, A R. (2007b). *Terrorism and surveillance: The technical and legal context*. New York, NY: Columbia University Press.

Weimann, G. (2006). *Terror on the internet*. Washington, DC: United States Institute for Peace.