

Copyright © 2007

## **The Challenges of Intelligence Sharing**

By  
Thomas B. Hunter  
December 2004

*Why has intelligence sharing and cooperation between diverse agencies and between different countries been so difficult? How could some of the major obstacles be overcome?*

### **Introduction**

Prior to the terrorist attacks on 9/11, problems with intelligence sharing among internal state agencies and on the international level were viewed primarily as functions of internecine territoriality or mistrusts lingering from a Cold War mindset. Following the attacks, however, both these agencies and state governments realized that failure to remedy these problems could potentially lead to such horrors being visited on their own soil. This new awareness was, no doubt, a direct result of the attacks themselves, which shattered the myth of America's invulnerability to major transnational terrorist attacks.<sup>1</sup>

The question obviously arose: if the most advanced, well-resourced, and ostensibly most powerful intelligence apparatus in the world failed to prevent these attacks, what would prevent these terrorists from conducting operations against less formidable opponents? The clear answer was that all states were and are vulnerable, particularly those with limited or flawed intelligence systems. The events of 9/11 caused some nations to rethink their existing apparatuses in order to improve intelligence sharing.

While counterterrorism has long been one aspect of modern intelligence, no single factor has motivated change and innovation in the international intelligence community<sup>2</sup> more than the specter of terrorism carried out against the 'homeland.' For that reason, this essay will focus on this dynamic and its relationship to national and international intelligence sharing. In this discussion, it is possible to also view how other elements of intelligence may fit into this equation.

This essay will also focus on US intelligence agencies as examples, for purposes of clarity and continuity. As the US agencies have equivalent counterparts in most countries, it is not a difficult endeavor to compare and contrast the similarities between those in the US and those of other nations. The challenges and potential solutions to intelligence sharing provided herein are not exclusive to the US, but rather representative of universal challenges faced by all nations.

### **Defining Intelligence and Intelligence Agencies**

Intelligence, such as that obtained and produced by the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI), is somewhat difficult to define, given the various missions for which various agencies are responsible. With a different focus comes a different definition. For purposes of this discussion, the author adopts the US Department of Defense (DoD) definition of intelligence as “information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.”<sup>3</sup>

Intelligence is usually obtained through a commonly understood system of collection methods. These include, but are not limited to the following<sup>4</sup>:

- HUMINT – Human-sourced Intelligence<sup>5</sup>
- SIGINT – Signals Intelligence<sup>6</sup>
- IMINT – Imagery intelligence<sup>7</sup>
- MASINT – Measurement and Signatures Intelligence<sup>8</sup>
- OSINT – Open Source Intelligence<sup>9</sup>
- Geospatial Intelligence<sup>10</sup>

Within any government, there are usually offices whose primary function it is to gather, assess, and disseminate intelligence for the state. For example, in the US, there are fifteen agencies, offices, or departments that make up the ‘Intelligence Community’.<sup>11</sup> In the UK, the lead agencies are MI5, MI6, and the Government Communications Headquarters (GCHQ).<sup>12</sup> Military intelligence is also a vital component of national security. In the US, this includes the Defense Intelligence Agency (DIA) and the various departments of the military services,<sup>13</sup> while in the UK this responsibility falls under the Defense Intelligence Staff (DIS) and elements of the military services.<sup>14</sup>

Thus, we can see that a state’s intelligence capabilities are not monolithic, but rather spread throughout a wide variety of civilian and military offices (at least in the case of developed nations with sufficient resources). These offices, of course, bring with them different missions and foci, which can sometimes bring them into conflict with one another.

### **Obstacles to Intelligence Sharing**

There are numerous reasons why agencies and nations fail to share information. With regard to agencies within a nation, these reasons tend to be of a territorial nature, with each agency striving to outdo the other in order to prove its worth, gain prestige and, more importantly, continued (or increased) funding from the federal budget. These reasons become more complicated as we consider the dynamics of international relations as they pertain to the conduct of states and concerns over security and sovereignty.

An aspect of intelligence sharing that must also be considered (and is shared by most nations with such capabilities) is the difference in missions between intelligence agencies, law enforcement, and the military. Intelligence agencies, such as the CIA in the US, commonly focus on external threats to the state, and provide finished intelligence assessments to policy makers. Law enforcement agencies, such as the FBI, exist primarily to confront domestic threats, but with a focus on forming criminal cases for later prosecution. Military intelligence, such as the DIA, shares a similar mission focus with state foreign intelligence agencies, in that they too are concerned over

external threats.<sup>15</sup> However, military intelligence also has as a priority providing actionable intelligence to its warfighters.

Thus, the differing missions, or motivations, of intelligence agencies can clearly be seen to vary greatly depending on that agency's focus. Where this variance can cause problems is when agencies become overly concerned with maintaining their exclusive access to intelligence. This territoriality, according to the *9/11 Commission Report*, contributed to the overall failings of US intelligence to predict or prevent those attacks.

Yet, while territoriality and interagency feuding are obstacles without reasonable merit, other related concerns are sometimes valid. For example, while the CIA may be interested in obtaining information held by the FBI on a given individual, the FBI may be reluctant to part with that information for fear that the CIA's use of that intelligence may compromise an ongoing investigation. Alternately, should the FBI seek information it believes to be held by the CIA, the CIA may be unwilling to provide that information over concerns that it may be demanded by a federal judge or somehow leaked to the public. Release of this intelligence, intentional or otherwise, to the public may lead to the capture or death of a source or to the exposure of an ongoing covert operation.

As mentioned previously, these dynamics are not limited to US intelligence agencies. The concerns over sharing information cited here are shared by agencies and departments in states around the world. This has led, no doubt, to failures in preventing terrorist attacks, locating terrorists, conducting effective criminal investigations, and other important responsibilities. Yet, while these problems may seem insurmountable, as entrenched and diametrically opposed as they appear, there are some potential solutions.

### **Overcoming Domestic Obstacles**

One factor that has hindered cooperation between US intelligence agencies for decades has been interagency rivalry, particularly between the CIA and FBI. Similar problems have existed between these two agencies and the Department of Defense, as well as with other government offices.

The US took one significant step forward following the 1993 bombing of the World Trade Center in New York City. FBI Director Louis Freeh ordered the creation of a new Counterterrorism Division to complement the CIA's Counterterrorism Center. He further arranged exchanges with senior FBI and CIA officials, and pushed for better cooperation between his legal attaches and CIA stations abroad. Yet, while this undoubtedly enhanced the relationship between the two agencies, the 9/11 Commission report cited Freeh's efforts "did not, however, translate into a significant shift of resources to counterterrorism."<sup>16</sup>

In February 2003, President Bush described increased cooperation between the FBI and CIA as "one of the greatest advantages in the war on terror."<sup>17</sup> However, in a more recent radio address to the nation, the president tacitly acknowledged that problems remain. When commenting on pending legislation that was intended to increase intelligence sharing, he stated:

The most important provisions of any new bill must create a strong, focused new management structure for our intelligence services and break down the

remaining walls that prevent the timely sharing of vital threat information among federal agencies and with relevant state, local, and private sector personnel.<sup>18</sup>

The proposed legislation would create, for the first time, a director of national intelligence to oversee all US intelligence efforts. Perhaps more importantly, the bill would also mandate the creation of a national counterterrorism center to coordinate all intelligence related to the war on terrorism.<sup>19</sup>

Following 9/11, both the US and the UK created new organizations specifically intended to merge the intelligence capabilities of various national agencies. These “fusion centers” soon expanded into other areas, to include law enforcement. Most notable among these are specialized task forces formed by the FBI to combat terrorism.

#### *Joint Terrorism Task Force (JTTF)*

In 1980, the FBI formed its first Joint Terrorism Task Force (JTTF) office. Following 9/11, the numbers of these offices increased dramatically with the new requirement for greater intelligence sharing. The purpose of these offices is to combine the intelligence capabilities of local and federal law enforcement in order to more efficiently and effectively track down terrorists.<sup>20</sup> There are currently 84 such offices in operation, including one in each of the FBI’s 56 main field offices, with plans to increase this total to 100 or more.<sup>21</sup>

In 2002, the FBI also created a National Joint Terrorism Task Force (NJTTF), based in its Washington, DC headquarters.<sup>22</sup> The NJTTF, which is comprised not only of FBI agents and analysts, but representatives from over 30 other agencies, is responsible for collecting terrorism information and intelligence and distributing it to the various JTTFs throughout the country.

#### *Terrorist Threat Integration Center (TTIC)*

The CIA has also been actively involved in the use of fusion centers. As part of his State of the Union address in January 2003, President Bush ordered the creation of the Terrorist Threat Integration Center (TTIC).<sup>23</sup> This new organization is comprised representatives from the CIA, DIA, FBI, National Security Agency (NSA), Department of Homeland Security, Department of State, Department of Defense, and other agencies.<sup>24</sup> Bolstering this joint effort was the relocation of the FBI’s Counterterrorism Division and CIA’s Counterterrorist Center (CTC) to the same building as TTIC in May 2004.<sup>25</sup>

Establishment of the TTIC was a direct result of the intelligence failures of 9/11 and the increased demands placed upon the US government to support the Global War on Terror. According to an official CIA press release,

TTIC officers are responsible for assessing, integrating, and expeditiously disseminating available threat information and analysis; maintaining an all-source database on known and suspected terrorists; and identifying collection requirements related to the terrorist threat.<sup>26</sup>

#### *Joint Terrorism Analysis Centre (JTAC)*

The UK provided another example of the proliferation of fusion centers with the establishment of the Joint Terrorism Analysis Center (JTAC) in June 2003.<sup>27</sup> The JTAC is comprised of representatives from eleven government departments and agencies and is responsible for analyzing and assessing intelligence relating to international terrorism.<sup>28</sup> The JTAC, as with the TTIC, produces finished intelligence for a wide variety of audiences.

The British government, like that of the US government, chose to include a wide range of diverse but related agencies and departments in their effort at improving intelligence fusion. Members of the JTAC include the Home Office, the Police, the Foreign and Commonwealth Office, the Ministry of Defence, the Department of Trade and Industry's Office for Civil Nuclear Security, and the Department for Transport's Security Department.<sup>29</sup>

In the cases of the US and UK examples, it is clear that these governments have acknowledged the need for inclusion, versus exclusion, of non-traditional players in the intelligence arena. This is an essential component of intelligence sharing due to the fact that these unconventional partnerships can offer previously untapped and unexploited resources.

Another excellent example is the US Interagency Intelligence Committee on Terrorism (IICT). The IICT consists of more than forty federal agencies, all of whom share a common interest in combating terrorism.<sup>30</sup> The group, which meets regularly to share information on terrorist issues, not only includes the major intelligence agencies, but includes law enforcement entities, such as the US Capitol Police.<sup>31</sup>

The primary beneficial result of these fusion centers and joint working groups is that instead of operating independently and being largely unaware of the capabilities and information held by other agencies, groups have an opportunity to express their requirements and to provide information. For example, sharing or shared databases can bring together information not previously amalgamated in one place for analysis. Information gathered by the US Citizenship and Immigration Services (USCIS),<sup>32</sup> such as documentation of the arrival of a foreign national at a port of entry, might be useful in developing a more comprehensive assessment of the movements of a terrorist group in the US. This information, shared regularly today, was not shared as readily in the years and months leading up to 9/11.

### **Problems with International Intelligence Sharing**

There are a number of important hurdles to face when nations consider sharing intelligence. The first of these is the potential for the compromise of information. Once a piece of intelligence leaves the hands of the providing state, there are no guarantees that it will be used responsibly and held in confidence.

Of concern to all intelligence agencies is the potential for the compromise of "sources and methods." Sources and methods are those means by which an intelligence agency gathers its information, such as via a human asset on the ground, a satellite in orbit, or the interception of a cellular telephone call. These sources and methods are, understandably, protected quite aggressively, especially if they are providing valuable intelligence that cannot be obtained through other means. It is not surprising, then, that

states would be reluctant to part with information that may, if misused, lead to the loss of that asset or the exposure of a previously classified capability.

This problem is exacerbated when a requesting agency is beset by its own internal problems. For example, the US may be hesitant to supply intelligence to the Pakistani Directorate of Inter-Services Intelligence (ISI) due to reports that elements within the ISI may be sympathetic to al-Qaida.<sup>33</sup> In these cases, the potential that intelligence may not only be misused, but used to aid an enemy, serves as an effective deterrent to sharing.

An additional concern is that shared intelligence may lead to human rights abuses or other misuses of provided information. Should the US, for example, provide intelligence to Egypt that led to the arrest, detention, and torture of an individual, and should this development be made public, the US would undoubtedly suffer accusations that it was intentionally complicit in this illegal activity.

Sometimes these problems are overcome by necessity. For example, a state may be motivated to provide intelligence to another state with the expectation that the “favor” will be reciprocated. Thus, there are times when states may have an incentive to share intelligence on specific issues. For example, the US may provide intelligence on Palestinian fund raising in the US, provided that Israel shares some of what it knows about the proliferation of manportable air defense weapons among Islamic extremists in Lebanon. However, these ad hoc arrangements are not long term solutions to the problems of intelligence sharing. Rather, they are relationships of necessity.

### **Overcoming Obstacles to International Intelligence Sharing**

The task of improving intelligence sharing among nations is, as previously mentioned, a matter of daunting proportions. This is not to say, however, that there is no potential for improvement, or indeed even some possible solutions.

Clearly, the most effective tool to date has been the formalization of intelligence sharing relationships. There are nations with which these concerns are alleviated through a history of intelligence sharing. Most notable among these is the special relationship between the US, UK, Canada, Australia, and New Zealand. This relationship was formalized in the UK/USA Security Agreement, the details of which remain classified.<sup>34</sup>

One idea that could facilitate intelligence sharing is the creation of an international intelligence integration center or centers. Similar to the fusion centers currently operating in the US and UK, it is possible that this concept may also be transferred to the international community. While the issues of secrecy and the myriad complexities of such an arrangement would be daunting, it is possible to envision such a system.

When considering such an institution, even hypothetically, there are several issues to be assessed. First, it seems logical that a new system of this type would inherently require a global presence. To facilitate this, numerous offices would be required, rather than simply one “headquarters”-type monolith based far from the areas of concern. The best way to address this would be the establishment of regional offices, located within the regions of their focus.<sup>35</sup> For example, a network of offices, with one each in Latin America, Western Europe, Eastern Europe, Asia, and the Middle East, would provide global coverage.

This type of dispersal would also offer the advantage of being able to coordinate locally with national intelligence agencies, particularly in times of crises. For example, in the case of a major terrorist attack in Saudi Arabia, the Middle East office (ostensibly with representatives from all neighboring states) could coordinate quickly to share intelligence on who may have been responsible, the numbers and nationalities of casualties, and information on possible follow-on attacks.

While this suggestion may indeed be utopian, the utility of such an apparatus appears sound. Clearly, and as stated previously, national concerns over security and sovereignty would create major hurdles to the creation of such a system. Moreover, rivalries and animosities (e.g. India/Pakistan, Iran/Iraq, Israel/Syria) may inhibit even a preliminary discussion of such partnerships. It is more likely that states which already share a friendly or neutral relationship would be induced to participate, if they do not already.

Another idea that may increase cooperation on an international level could be the formation of issue-specific working groups. For example, the creation of a permanent group of Middle Eastern nations (with participation from other relevant states such as the US) could be beneficial in discussing developments in terrorist fundraising in the region. If formalized and scheduled on a regular basis (e.g. bimonthly), such an arrangement could help keep all member nations apprised of current developments in these types of issue-specific areas.

## **Conclusions**

There is no panacea for the challenges presented by intelligence sharing, either domestically or internationally. There are, however, steps that states can take to improve on the agreements and understandings currently in place. These may be ad hoc, temporary solutions, or long-term arrangements to create permanent systems for intelligence sharing.

Any improvements in these areas will be easier to produce domestically, where agencies and departments ostensibly fall under the guidance of one government body. In these cases, changes can be made at senior levels with the knowledge that given recommendations are mandatory, and must be carried out. Also, these entities usually have a common end goal, which is ensuring the security of the state. Thus, improvements in intelligence sharing are easier to make at home than they are when other nations are brought into the mix.

As mentioned previously, some of these steps have been taken already, and have proven successful. In the case of the US example, these include fusion centers (e.g. TTIC, JTTFs) and permanent joint meeting groups (e.g. IICT). Further possible improvements could include the creation of a permanent "intelligence czar" to oversee the whole of a state's intelligence community, with the authority to implement needed changes (including budgetary authority), despite potential institutional resistance.

When considering improvements in international intelligence sharing, the problems are much more diverse and difficult. Nonetheless, there are ways, both old and new, in which this problem might be mitigated. Formalized intelligence sharing agreements, the creation of international intelligence integration centers, and issue-specific task forces

are all means by which states might enhance their willingness and ability to share intelligence.

Certainly, there are numerous hurdles that must be overcome, not the least of which is trust. This factor may prove the most difficult of all challenges facing those states which seek to increase cooperation. However, just as states united to share intelligence during the Cold War, it is possible that the new threat of transnational terrorism may force states to reconsider old biases and feuds in order to improve domestic security.

Copyright © 2007

## APPENDIX A

### **Internet Resources: Selected International Intelligence Agencies**

#### Australia

Australian Secret Intelligence Service (ASIS) <http://www.asis.gov.au/>

Australian Security Intelligence Organization (ASIO) <http://www.asio.gov.au/>

#### Canada

Canadian Security Intelligence Service (CSIS) <http://www.csis-scrs.gc.ca/>

Communications Security Establishment (CSE) <http://www.cse.dnd.ca/>

#### Israel

The Institute for Intelligence and Special Tasks (Mossad)  
<http://www.mossad.gov.il/>

#### New Zealand

New Zealand Security Intelligence Service (NZSIS) <http://www.nzsis.govt.nz/>

#### Russia

Federal Security Service (FSB) <http://www.fsb.ru/>

Foreign Intelligence Service (SVR) <http://svr.gov.ru/>

#### United States

Central Intelligence Agency (CIA): <http://www.cia.gov/>

Defense Intelligence Agency (DIA): <http://www.dia.mil/>

Federal Bureau of Investigation (FBI): <http://www.fbi.gov/>

National Security Agency (NSA) <http://www.nsa.gov/>

#### United Kingdom

Defence Intelligence Staff (DIS): <http://www.mod.uk/dis/>

Government Communications Headquarters (GCHQ): <http://www.gchq.gov.uk>

MI5 (Security Services): <http://www.mi5.gov.uk>

MI6 (Secret Intelligence Service): <http://www.fco.gov.uk/sis>

## Selected Bibliography

- Anonymous, Imperial Hubris: Why the West is Losing the War on Terror (USA: Brassey's Inc., 2004)
- Buckley, Mary and Fawn, Rick (eds.), Global Responses to Terrorism: 9/11, Afghanistan and Beyond (London: Routledge, 2003)
- Cassese, Antonio, Violence and Law in the Modern Age (Princeton, New Jersey: Princeton University Press, 1986)
- Corbin, Jane, The Base: Al-Qaeda and the Changing Face of Global Terror (Great Britain: Pocket Books, 2003)
- Godson, Ray (et al), US Intelligence at the Crossroads: Agendas for Reform (UK: Brassey's UK Ltd., 1995)
- Harclerode, Peter, Fighting Dirty: The Inside Story of Covert Operations from Ho Chi Minh to Osama bin Ladin (London: Cassell & Co., 2001)
- Mark, Sir Robert, Policing a Perplexed Society (London: William Clowes & Sons, Ltd., 1977)
- National Commission on Terrorist Attacks, The 9/11 Commission Report: The Final Report of the National Commission on Terrorist Attacks (USA: W.W. Norton & Company, 2004)
- Pillar, Paul R., Terrorism and U.S. Foreign Policy (Washington, D.C.: Brookings Institution Press, 2001)
- Rubin, Barry, The Politics of Counterterrorism: The Ordeal of Democratic States (Washington, D.C.: University Press of America, 1990)
- Turner, Stansfield, Secrecy and Democracy (London: Sidgwick & Jackson Ltd., 1985)
- Walker, Clive, Blackstone's Guide to the Anti-Terrorism Legislation (Oxford: Oxford University Press, 2002)
- Wilkinson, Paul, Terrorism Versus Democracy: The Liberal State Response (USA: Frank Cass, 2005)

---

<sup>1</sup> While the US had experienced a major domestic terrorist attack with the truck bombing of the Alfred P. Murrah Federal Building in Oklahoma City in 1995, a dramatic and successful attack by transnational actors had yet failed to materialize. Al-Qaida's targeting of the World Trade Center in 1993, while

---

resulting in some casualties and causing significant damage to the underground parking area, failed to topple the building(s), and thus did not provide the same societal impact as the 9/11 operations.

<sup>2</sup> The concept of an international intelligence community is presented here not as a formal regime, but rather as a collective term used to describe international intelligence agencies and departments, particularly with regard to their interaction within the international community.

<sup>3</sup> *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (as amended through October 7, 2004), pg. 263.

<sup>4</sup> A detailed discussion of these collection methods is beyond the scope of this paper, but brief definitions of each of these methods are provided in these endnotes to provide a basic understanding of the myriad ways in which intelligence is collected. These definitions also provide a deeper understanding of the potential conflicts which may arise between intelligence agencies when it pertains to sharing this intelligence. Definitions for each were derived from the US Intelligence Community official website. While these definitions discuss, in part, how each is utilized within the US system, these terms are not specific to the US, and indeed are shared by all nations with an intelligence gathering capability. See [http://www.intelligence.gov/2-business\\_cycle2.shtml](http://www.intelligence.gov/2-business_cycle2.shtml).

<sup>5</sup> Human Intelligence is derived from human sources. To the public, HUMINT remains synonymous with espionage and clandestine activities, yet, in reality, most HUMINT collection is performed by overt collectors such as diplomats and military attaches. HUMINT is the oldest method for collecting information, and until the technical revolution of the mid to late twentieth century, it was the primary source of intelligence. HUMINT is used mainly by the CIA, the Department of State, the DoD, and the FBI. Collection includes clandestine acquisition of photography, documents, and other material; overt collection by personnel in diplomatic and consular posts; debriefing of foreign nationals and US citizens who travel abroad; and official contacts with foreign governments. The National HUMINT Requirements Tasking Center is responsible for providing guidance for HUMINT activities, which are reflected in the National HUMINT Collection Directive. As part of this national effort, all HUMINT collection within the DoD is managed by the Defense HUMINT Service, under the direction of DIA's Directorate for Operations.

<sup>6</sup> Signals Intelligence is derived from signal intercepts comprising -- however transmitted -- either individually or in combination: all communications intelligence (COMINT); electronic intelligence (ELINT); foreign instrumentation signals intelligence (FISINT). The NSA is responsible for collecting, processing, and reporting SIGINT. The National SIGINT Committee within NSA advises the Director, NSA, and the DCI on SIGINT policy issues and manages the SIGINT requirements system.

<sup>7</sup> Imagery Intelligence includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. NGA is the manager for all imagery intelligence activities, both classified and unclassified, within the government, including requirements, collection, processing, exploitation, dissemination, archiving, and retrieval.

<sup>8</sup> Measurement and Signature Intelligence is technically derived intelligence data other than imagery and SIGINT. The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. Examples of this might be the distinctive radar signatures of specific aircraft systems or the chemical composition of air and water samples. The Central MASINT Organization, a component of DIA, is the focus for all national and DoD MASINT matters.

<sup>9</sup> Open-Source Intelligence is publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings. While open-source collection responsibilities are broadly distributed through the IC, the major collectors are the Foreign Broadcast Information Service (FBIS) and the National Air Intelligence Center (NAIC).

<sup>10</sup> Geospatial Intelligence is the analysis and visual representation of security related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information.

<sup>11</sup> The US Intelligence Community is made up of the following governmental bodies: Central Intelligence Agency; Defense Intelligence Agency; National Security Agency; National Geospatial Intelligence Agency (formerly the National Imagery and Mapping Agency, or NIMA); National Reconnaissance Office; Army Intelligence; Navy Intelligence; Air Force Intelligence, Surveillance, and Reconnaissance; Marine Corps

---

Intelligence; Department of Homeland Security; Federal Bureau of Investigation; Department of the Treasury; Department of Energy; and Department of State.

<sup>12</sup> A brief summation of the duties of these agencies is beneficial to this discussion. In the UK, MI5, also known as the Security Services, is roughly equivalent to the US FBI. It provides domestic intelligence services against “covertly organized threats to national security...(including) terrorism and the proliferation of weapons of mass destruction.” MI6, also known as the Secret Intelligence Service (SIS) is equivalent to the US CIA in role and mission. According to official British information, MI6 is “responsible for obtaining secret information and conducting operations in support of the UK’s foreign policy objectives, and to counter threats to UK interests worldwide.” GCHQ, the third of the three primary UK intelligence services, is similar to the US NSA, in that it is responsible for gathering SIGINT around the world on behalf of the government.

<sup>13</sup> Within the US military there are four primary services, the Air Force, Army, Navy, and Marine Corps. In times of war, the US Coast Guard falls under the control of the US Navy. All five of these elements have their own intelligence capabilities which are collectively subordinate to the Department of Defense and the Joint Chiefs of Staff.

<sup>14</sup> Please Appendix A for select guide to international intelligence agencies that can be found on the internet.

<sup>15</sup> <http://www.dia.mil/This/Intro/index.html>

<sup>16</sup> The National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, July 22, 2004, pg. 76.

<sup>17</sup> <http://www.whitehouse.gov/news/releases/2003/02/20030214-5.html>.

<sup>18</sup> <http://www.whitehouse.gov/news/releases/2004/12/20041204.html>

<sup>19</sup> <http://www.washingtonpost.com/wp-dyn/articles/A35205-2004Dec4.html?nav=headlines>

<sup>20</sup> <http://www.fbi.gov/terrorinfo/counterrorism/partnership.htm>.

<sup>21</sup> For further information on the NJTTF, see interview with Acting Chief Ken Love. This interview also provides insight into the utility of fusion centers in intelligence sharing.

<http://www.fbi.gov/page2/july04/njtff070204.htm>

<sup>22</sup> Ibid.

<sup>23</sup> <http://www.whitehouse.gov/news/releases/2003/01/20030128-19.html>.

<sup>24</sup> [http://www.cia.gov/cia/public\\_affairs/press\\_release/2003/pr05012003.html](http://www.cia.gov/cia/public_affairs/press_release/2003/pr05012003.html).

<sup>25</sup> Ibid.

<sup>26</sup> Ibid.

<sup>27</sup> <http://www.cabinetoffice.gov.uk/publications/reports/intelligence/govres2003.pdf>.

<sup>28</sup> <http://www.mi5.gov.uk/output/Page65.html>

<sup>29</sup> Ibid.

<sup>30</sup> Paul R. Pillar, *Terrorism and U.S. Foreign Policy* (Washington, D.C.: Brookings Institution Press, 2001), pg. 124.

<sup>31</sup> The inclusion of law enforcement agencies, particularly on the local level, is a largely untapped resource in domestic intelligence sharing. Given their unique ability to provide information on criminal activity, particularly with regard to specific individuals who may be suspected of supporting terrorism, police forces offer a unique capability that cannot be duplicated by federal agencies. For a discussion of the relationship between police and the military, for example, see Sir Robert Marks, *Policing a Perplexed Society* (London: William Clowes & Sons, Ltd., 1977), pgs. 23-33.

<sup>32</sup> The USCIS was formerly known as the Immigration and Naturalization Service (INS). The INS was disbanded as part of the Homeland Security Act of 2002, and the USCIS now falls under the jurisdiction of the Department of Homeland Security (DHS). For further information see the organization’s official website at <http://www.uscis.gov>.

<sup>33</sup> For discussions of possible complicity with al-Qaida, see Arnaud de Borchgrave, “Al-Qaida’s Privileged Sanctuary,” June 17, 2002 (<http://www.upi.com/view.cfm?StoryID=17062002-043525-4513r>); Michael Meacher, “The Pakistan Connection,” *Guardian Unlimited*, July 22, 2004

(<http://www.upi.com/view.cfm?StoryID=17062002-043525-4513r>); and “U.S.: Bin Ladin’s Whereabouts Remain Mystery,” February 24, 2002, <http://edition.cnn.com/2002/US/02/24/gen.bin.laden/index.html>.

---

<sup>34</sup> Philip Rosen, “The Communications Security Establishment – Canada’s Most Secret Intelligence Agency,” Parliamentary Information and Research Service, September 1993.  
<http://www.parl.gc.ca/information/library/PRBpubs/bp343-e.htm>

<sup>35</sup> Existing intelligence sharing agreements between nations, such as those in Europe, may be considered by some to be sufficient to address such events as they occur within Europe. However, as terrorism takes on an increasingly transnational nature, it is no longer sufficient for states to rely exclusively on these existing, regional security relationships to gather, assess, and relevant intelligence.

Copyright © 2007