

International Cooperation of Intelligence Agencies against Transnational Terrorist Targets

Katarina Zivanovic *

Introduction

In the post-9/11 world, the role of intelligence agencies has continued to evolve. The most notable change from the Cold War environment, which was characterized by a lack of information sharing, has been the new emphasis on cooperation between intelligence agencies. It has become critical in this new environment for the intelligence community to change its ways, but this has not necessarily come easily. This essay will examine how the structure of threats has changed in today's world, and will address the shift in attitudes toward cooperation throughout the international intelligence community.

The ancient Chinese strategist Sun Tzu wrote over two thousand years ago that if you “know the enemy and know yourself, in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal.”¹ The need for intelligence activities developed along with the evolution of human society and military activity. The desire to overtake and conquer an opponent and protect one's own interests created an environment where one always needed to have more knowledge about one's opponent, in order to discover his weaknesses and strengths. Even though we can not identify precisely the exact moment of the birth of intelligence activity, we can find in various historical sources that powerful rulers in Africa and Asia were sending delegates to neighboring countries to collect information as early as the seventh century B.C. Rodger Hillman reminds us that the first written data on intelligence activities can be found in the Old Testament, when Moses sent spies to gather information about the land of Canaan.²

Many authors would agree that the competing interests at work—economic, social, political, military, etc.—in the process of building a state were the main reasons for creating a notion of secrecy that became an integral part of international relations. Different groups had different interests that were opposed to each other. The main task was to protect each group's “secrets” in order to maintain position and disguise intentions; through discovering somebody else's secrets, it was hoped that you would be

* Katarina Zivanovic, a 2007 graduate of the George C. Marshall European Center for Security Studies, works in the General Directorate for NATO and Defense Affairs of the Ministry of Foreign Affairs of the Republic of Serbia, in charge of international security and terrorism issues. The views expressed in the research paper are her personal views and do not in any way represent the official position of the government of the Republic of Serbia.

¹ Sun Tzu, *The Art of War*, trans. Samuel B. Griffin (New York: Oxford University Press, 1963), 84.

² See the Book of Numbers, Ch. 13; M.P. Milashinovich, *Terror of the West Over Modern Society* (Belgrade: BIGZ, 1997).

able to better achieve your own goals. The roots of intelligence agencies can be found in the struggle of opposing interests as a means to gain superiority.³

Wars played a crucial role in the development of intelligence agencies. The more you knew about your opponent, his military organization, and his strategic intentions, the greater your chances for victory. In Mongolia during the period of Genghis Khan, an intensive level of intelligence activity was developed, practiced not only by legates and traders, but by permanent agents as well.⁴

The intelligence agency, as the institutional home of such activity, appeared during the emergence of centralized states under absolute monarchies. Venice had the strongest intelligence agency in the sixteenth and seventeenth centuries, and some authors consider it to be the root of modern intelligence agencies.⁵ More rapid and comprehensive development of intelligence agencies came during the nineteenth and twentieth centuries, especially in the period between the two World Wars. The classic methods of intelligence work were refined at that time, and they became the basis of a new strategic approach in international relations. After World War II and during the Cold War there was a plethora of conflicting state interests in different areas—politics, diplomacy, culture, science and technology—where intelligence activity took on new dimensions. All processes in all areas of social life became zones of intelligence interests. Thus, in their initial stages of development, intelligence activities were used by different groups, classes, parties, and individuals within a ‘state.’ Later, however, they became a critical instrument for accomplishing the vital interests of nation-states.⁶

How Intelligence Works

What is intelligence? People have different definitions of the term. Some see it as classic “cloak and dagger” activity, along the lines of international spycraft. Others see it as a form of “Big Brother” surveillance, by which an all-powerful state monitors the activities of its citizens. For a soldier it can be knowledge of the enemy over the horizon; analysts see it as information that is waiting for clarification; and policymakers consider it to be information that meets stated or understood needs. Intelligence includes all the elements that gather together under the umbrella of national security, defense, and foreign policy, as well as certain aspects of international security. According to Melanie M.H. Gutjahr, intelligence is the process by which specific types of information that are important to national security are requested, collected, analyzed, and provided to policymakers. Intelligence is also the product of that process, the safeguarding of these processes and the respective information from counterintelligence activities, and the carrying out of operations as requested by lawful authorities.⁷

³ *Military Encyclopedia*, vol. VI, 2nd edition (Belgrade, 1973), 215.

⁴ Adam Purg, *Obvescevalne sluzbe* (Ljubljana: Enotnost, 1995), 7.

⁵ *Ibid.*, 14.

⁶ For a thorough history, see Purg, *Obvescevalne sluzbe*.

⁷ Melanie M.H. Gutjahr, *The Intelligence Archipelago: The Community's Struggle to Reform in the Globalized Era* (Washington, D.C.: Joint Military Intelligence College, May 2005).

The aim of intelligence activities in the current moment is determined by the transformation of intelligence interests and the objects of their interest, and it has had an influence on the development of intelligence agencies. Today, these agencies are trying to prevent surprises, make predictive and expedient decisions, and provide for the efficient conduct of state systems and command over the armed forces.⁸

Assignments of intelligence activities follow from the constantly changing needs of various leaders. Those needs are translated into demands for information on trends and conditions in specific sectors of society or in a society as a whole, as well as on relations between states in the international arena. Intelligence activities involve several phases: collection; processing; exploitation; analysis and production; dissemination and consumption; and feedback.⁹

Collection

There are various types of intelligence collection; sometimes they are called the “collection disciplines,” or “INTs.” Technical collection systems are usually very expensive. Therefore, the ability to operate a large number of collection systems at the same time will always be constrained by costs. No single method of collection is used in isolation. Very often the details of collection capabilities (and even the existence of some of them) are highly classified secrets.¹⁰

The collection disciplines include a variety of different approaches. Imagery intelligence (IMINT) is derived from airborne and space collection platforms, such as satellites and aircraft. In the 1960s and 1970s, PHOTINT (photo intelligence) was the mainstay of IMINT. Signals intelligence, or SIGINT, refers to communication intercepts, and is a product of a number of subsidiary collection disciplines. Communication intelligence (COMINT) is the main source of SIGINT. Electronic intelligence (ELINT) contributes to SIGINT by gathering information from telephones, fax machines, copiers, and other electronic devices. Telemetry intelligence (TELINT) refers to the interception of encrypted signals. Measurement and signature intelligence (MASINT) employs resources of both IMINT and SIGINT. It is a relatively new discipline, and refers to weapons capabilities and industrial activities (for example, it can help identify the types of gases or wastes leaving a factory, which can be extremely important in chemical weapon identification). Human intelligence (HUMINT) relies less on technology and more on human labor. It involves sending agents to foreign countries, where they try to recruit foreign nationals to engage in espionage. Some intelligence targets, such as terrorism, international crime, or narcotics trafficking are

⁸ Interview with Prof. John Le Beau, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

⁹ Milan Delic, *Obavestajna delatnost* (Belgrade: MUP RS, 1996).

¹⁰ This discussion on collection methods is based on the work of Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2000), and the lectures by Prof. John Le Beau in his seminar on “Intelligence Challenges for Democratic States,” held in November 2007 at the George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany.

difficult to deal with by technical means or through technical disciplines. In some instances, HUMINT may be the only available source of intelligence. It is also far less expensive than technical intelligence, but is very liable to deception. A new form of intelligence collection—open source intelligence (OSINT)—is now considered by many intelligence officials to be a potentially rich vein of information. OSINT includes media (newspapers, radio, TV, Internet), public data (government reports, speeches, conference proceedings), and professional and academic products (conferences, symposia, academic papers).

Analysis

Analysis is the heart of the intelligence process. As Michael A. Turner argues, “Collecting intelligence information is of little value unless someone corroborates and evaluates the information, [then] sets it into context and uses it to form a series of judgments about foreign capabilities and intentions.”¹¹ Analysis exists in order to make sense of the secret world of intelligence and to communicate those insights to senior decision makers. The job of an analyst is to gather and collate all relevant intelligence information, analyze it for relevance and significance, and then draft reports for senior intelligence officials and policymakers. There are two forms of analytic reports: current intelligence (e.g., the “President’s daily intelligence briefing” by the CIA), and long-term research. Current intelligence deals with daily issues, while long-term research reports are forward-looking assessments of what might happen.

Counter-intelligence

Counter-intelligence is an effort taken to protect one’s own intelligence operations from penetration and disruption by hostile nations and their intelligence services.¹² It is both analytical and operational. There are three types of counter-intelligence:

- *Collection*: gaining information about an opponent’s intelligence capabilities that may be aimed at you
- *Defensive*: preventing hostile intelligence services from penetrating your intelligence agencies
- *Offensive*: identifying an opponent’s efforts against your systems and trying to manipulate these attacks, either by ‘turning’ opponents’ agents into double agents or by giving them false information.

Covert Action

This is one of the most controversial aspects of the intelligence realm. Covert action should not be undertaken solely at the initiative of the intelligence agencies. The United States’ National Security Act, Section 503(e) and Section 413b(e) of the United

¹¹ This section is derived from Michael A. Turner, *Why Secret Intelligence Fails* (Dulles, VA: Potomac Books, 2005), and the lectures by Prof. John Le Beau mentioned above.

¹² For further information on counter-intelligence, see Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2000).

States Code define covert action as “an activity or activities by the United States government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States government will not be apparent or acknowledged publicly.”¹³

The Role of the Policymaker

Intelligence has always played a critical role for policymakers in the process of setting the course for a state’s domestic and foreign policy. As Mark Lowenthal has written, there is a constant need for intelligence that will provide background, context, information, warning, and assessments of risks, benefits, and likely outcomes for policymakers. But there should be a clear line drawn between intelligence and policy. Intelligence can play only a supporting role, and may not cross over into advocacy for specific policies. If there is a strong preference for a specific policy outcome, the intelligence analysis that is carried out may have a similar bias. That is called “politicized intelligence.” There are three important caveats in this regard:

- A distinction between policymakers and intelligence operatives does not mean that intelligence officers do not care about policy outcomes and do not influence them. We must make a distinction between an attempt to influence the process by providing acceptable intelligence and trying to manipulate intelligence so that policymakers make a specific choice. The latter case is not acceptable.
- Senior policymakers can and do ask senior intelligence officials for their opinions.
- Policymakers can reject or ignore intelligence at any moment.¹⁴

Nevertheless, if we look at the position and role that modern intelligence agencies play in the international arena, we can advance the hypothesis that the activities of intelligence agencies are part of the official policies of their states. If we keep in mind the fact that intelligence agencies, as specialized institutions, are part of the organizational system of a state that are guided by the top policymakers of the country, it is self-evident that their entire organization, planning, and activity should be strictly harmonized with that state’s political goals and tasks. Decision makers in many situations depend on intelligence analysis, assessments, and other products – this is how intelligence agencies exert immediate influence on the decision-making process within a state. Intelligence systems have a monopoly on the most delicate information, which gives them the power to influence the content and scope of decisions. They also have significant influence on all recipients of that information at all levels and phases of the process of the realization of state policy. In order to understand the essence of the relationship between intelligence and politics, it is necessary to know the basic elements of the politics of the respective countries involved.

¹³ See www.intelligence.gov/0-natsecact_1947.shtml.

¹⁴ Ibid.

The New Challenge of International Terrorism

During the Cold War, the international community was divided into two separate blocs that were completely at odds with one another, and therefore in constant tension. No state felt entirely secure at that time, but somehow, states felt secure in their insecurity. They knew exactly who their enemy was; how strong it was; and what its interests and goals were. The threat was precise and predictable. There were two blocs, two great powers that opposed each other and were in constant need of increasing their raw military power. International policies revolved around their interests; hence, one always knew what could be expected. Security could be measured exactly. One could even predict who would win in a direct clash by calculating and measuring the military power of the adversaries. That is perhaps one of the reasons why direct conflict between the United States and Russia never actually occurred during the Cold War: their power was estimated as being roughly equivalent. For Western countries, the most menacing threat to their national security was the growing influence and power of their ideological competitor, the Soviet Union, and ultimately its arsenal of ballistic missiles. The world was divided into Communist and non-Communist states, so for virtually every nation in the world the enemy was well-defined and organized, with a vast military apparatus.¹⁵

Intelligence agencies were traditional as well. Their tasks and structures were largely similar, no matter which country they belonged to. They were large, formal bodies with major budgets. Technology played a crucially important role (U-2 spy planes, satellites, sensors, cameras, etc.), and a significant percentage of each side's intelligence budget was dedicated to the improvement of technology. The major powers had a global intelligence reach; hence the intelligence struggle became global. A primary focus of both Eastern and Western intelligence services was the opposition's intelligence service ("spy vs. spy"). The main intelligence methods used during the Cold War were: recruitment of human sources; encouraging the defection of officials (for example, Stalin's daughter Svetlana defected from the USSR to the U.S., and was connected to the CIA thereafter); and special operations.¹⁶

After the Cold War, intelligence agencies lost their primary purpose for existence. They no longer had a priority target, only several small, so-called "flavor of the month" targets that were constantly changing. It was clear that they needed to redefine their missions.

Globalization has brought additional challenges. The distinction between military actions and criminal activities—in fact, between states of peace and war—has become

¹⁵ For more on the differences between the two international systems (i.e., the Cold War era and the post-Cold War era) see Joseph S. Nye, Jr., *Understanding International Conflicts*, 5th edition (New York: Longman, 2005); Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Farrar, Straus and Giroux, 1999); and Henry Kissinger, *Does America Need a Foreign Policy?* (New York: Simon & Schuster, 2001).

¹⁶ This section draws on the lectures delivered by Prof. John Le Beau in his seminar on "Intelligence Challenges for Democratic States" cited above.

blurred in today's world. The new enemy, no longer attached to a large, predictable state apparatus, has proven it can slip into and out of our nations undetected, reside unnoticed, move money invisibly, and communicate unhindered via everyday means with leadership elements located thousands of miles away. This enemy is not easily defined or identified, which complicates the situation for military and intelligence planners.¹⁷ Nevertheless, after the terrorist attacks on Washington and New York on 11 September 2001, it was absolutely clear that the world was never going to be the same, and that it faced something new, something for which intelligence organizations as they stood at the time were ill-prepared.

The threat of international terrorism has become a priority for the intelligence organizations of several countries, not just the United States. On 17 March 1992, a suicide bomber crashed an explosive-filled truck into the Israeli Embassy in Buenos Aires (twenty-nine people were killed, and hundreds more injured). Two years later, Buenos Aires was again hit with a terror attack. This time the target was the Jewish community center in the heart of the city (eighty-five were killed). After a full-scale investigation, it was clear that Hezbollah had carried out the attacks, but also that at least one of them was planned in Iran at the highest levels of the Iranian government, aided by a sophisticated sleeper-cell network in Latin America. The reason for the attacks was to punish the Argentine government for canceling some agreements with Iran and to send a warning to the rest of Latin America. Also, by focusing on soft targets in Jewish communities, the operation would serve an additional objective: demonstrating to Israel that Hezbollah could strike anywhere, at any time.¹⁸ As we can see in these examples, multiple organizations from several countries and two different continents were involved.

How can we deal with threats of this kind? Is one country able to address such a challenge on its own? What role does intelligence play in this security environment? What is new in the nature of this threat? Are we facing a new enemy? How does this new threat challenge intelligence organizations? First, we are facing a non-state actor that poses a global threat. It is very difficult to locate and understand its nature. Terrorist organizations span the globe with a great number of small cells. It is very difficult to monitor them by satellite or to track their communication systems. They operate clandestinely; most of the meetings where they discuss their plans are held in hotel rooms or apartments that are difficult to spy on. They do not draw attention to themselves. As one security analyst has noted, "Religious conviction gives them strength, but the armed struggle is what holds them together."¹⁹ Furthermore, "they measure success differently: They define death and destruction as achievements in themselves."²⁰ Also, "the frequent use of ever-changing actors, aliases, and code words is another

¹⁷ Ibid.

¹⁸ Dan Senor, "The Long Arm of Iran," *Wall Street Journal* (Eastern edition) (29 September 2007): A8.

¹⁹ Brian M. Jenkins, *Countering Al Qaeda* (Santa Monica, CA: Rand Corporation, 2002); available at www.rand.org/pubs/monograph_reports/2005/MR1620.pdf.

²⁰ Ibid.

unique challenge and significantly increases the chance of confusion and incorrect assessments.”²¹ The nature of terrorist behavior is the reason why intelligence agencies are facing so many challenges in combating the threat. Terrorists are very disciplined, dedicated, and highly motivated. They will not easily betray their cause. The variety of ways they conduct their operations results in the fact that it is very difficult to predict future targets.

Even trends in terrorism are not easy to define. As former CIA director George Tenet stated before Congress, “While we often talk of two trends in terrorism—state-supported and independent—in Bin Laden’s case with the Taliban we had something completely new: a *terrorist* sponsoring a *state*.”²² As the events of 9/11 indicated, existing intelligence structures were not ready for the new threat. It required them to adapt to a new set of international realities, but the problem was that intelligence structures were not created for adaptation.

Intelligence agencies in democratic states of the twenty-first century are dedicated to confronting transnational targets and non-state actors. The primary focus of most intelligence agencies, especially in the United States (the nation that has been most directly affected by these new threats) is on international terrorism and the proliferation of weapons of mass destruction (WMD), and on a concern that one day these weapons might fall into the hands of terrorist groups.²³

The first major intelligence act in the United States in fifty years—one that has changed the authorities conferred by the National Security Act of 1947—is the Intelligence Reform and Terrorism Prevention Act (17 December 2004). The fact is that nobody, including the intelligence agencies themselves, noticed that they needed reform.²⁴ Only after the attacks of September 11 did it become a pressing issue. The 9/11 Commission Report (*The Report of the National Commission on Terrorist Attacks Upon the United States*) stated that the United States intelligence community was poorly positioned to anticipate the emerging Al Qaeda threat and to deal with it on time.²⁵ The commission especially faulted the poor level of cooperation between the FBI and the CIA, given that considerable information was either not shared at all, or was shared very inefficiently. The biggest organizational change was the creation of a new position—the Director of National Intelligence (DNI)—who became the “one voice” of the intelligence community. He has overall responsibility for the entire

²¹ Kie C. Fallis, *Statement for the Record: Lessons Learned and Actions Taken in Past Events*, Report to Congress (8 October 2002), 5; available at www.fas.org/irp/congress/2002_hr/100802fallis.pdf.

²² George Tenet, *Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee* (17 October 2002), 4–5; available at https://www.cia.gov/news-information/speeches-testimony/2002/dci_testimony_10172002.html.

²³ Prof. John Le Beau, seminar on “Intelligence Challenges for Democratic States,” November 2007.

²⁴ *Ibid.*

²⁵ *The 9/11 Commission Report: Executive Summary* (Washington, D.C.: U.S. Government Printing Office, 2004), 1–26; available at www.gpoaccess.gov/911.

United States intelligence community (sixteen agencies), but lacks any operational authority.²⁶

Interestingly, following the July 2005 attacks on the London transit system, similar charges were leveled against the intelligence and law enforcement organizations of the United Kingdom. A significant effort was dedicated to trying to improve the intelligence agencies involved, especially their ability to collect and analyze intelligence on terrorist organizations in order to prevent attacks (although the Antiterrorism, Crime, and Security Act had already been passed in December 2001 in the wake of the 9/11 attacks on the U.S.).²⁷ Significant steps have also been made in Germany. Before September 2001 there was very little cooperation among the various German intelligence agencies. There were, in fact, distinct boundaries and walls between them. After 9/11, these boundaries became porous, and a coordinating body was founded. It has not been very efficient so far, but it nevertheless represents an important step forward.²⁸

The threat of the proliferation of WMD and the possibility of these weapons being in a terrorist's possession is currently one of the main preoccupations of intelligence agencies around the world. The development and production of WMD is very hard to track. Very small amounts of different substances that can be produced in small laboratories could be sufficient to cause massive destruction. Technical instructions for preparing such weapons can be found on the Internet.²⁹ Of particularly great concern is Al Qaeda's interest in acquiring unconventional weapons (WMD as well as chemical or biological elements). As one scholar has observed, "In a December 1998 interview, Bin Laden called the acquisition of these weapons a 'religious duty' and noted, 'How we would use them is up to us.'"³⁰

Pakistan, being the only nuclear-armed Muslim nation, is also currently a source of grave concern. Given the current level of political uncertainty in Pakistan, there is a possibility that rising instability could lead to the loss of a nuclear device or material. There is also the possibility that Pakistani scientists or security officials could take advantage of the unsettled conditions in their country by selling technology, supplies, or secrets to the highest bidder. According to reporting in the *Los Angeles Times*, "In 2001, just weeks before the 9/11 attacks, two Pakistani nuclear experts met with Osama bin Laden in Afghanistan to discuss how Al Qaeda should go about building a

²⁶ Prof. John Le Beau, seminar on "Intelligence Challenges for Democratic States," November 2007.

²⁷ *Antiterrorism, Crime, and Security Act of 2001*; available at http://www.opsi.gov.uk/acts/acts2001/ukpga_20010024_en_1.

²⁸ Prof. John Le Beau, seminar on "Intelligence Challenges for Democratic States," November 2007.

²⁹ Interview with Prof. John Le Beau, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

³⁰ Tenet, *Written Statement for the Record*, 5. For further research see Peter Katonah, Michael D. Intriligator, and John P. Sullivan, *Countering Terrorism and WMD: Creating a Global Counter-terrorism Network* (New York: Taylor & Francis Group, 2006).

nuclear device.”³¹ Al Qaeda may also strike with a “dirty bomb,” a device that would use conventional explosives to spew radioactive material into the air. There is a possibility that terrorists could come into possession of the deadly poison ricin, which was found in the rented apartment of four Algerians in Great Britain.³²

Collection

The collection of intelligence refers to the act of gathering information from technical means, satellites, human espionage, and other sources. Throughout the twentieth century, the national security concerns of most countries were largely focused outwards, on foreign governments and militaries. During the Cold War, spies were easily recruited, whether lured by money or driven by disillusionment with their nation’s ideology.³³

Huge sums of money were spent on developing and fielding unobtrusive imagery and signals control platforms and other technologies in order to closely monitor subjects and gain intelligence directly from locations overseas. But even being physically on the ground with sophisticated equipment cannot penetrate into the enemy’s mind, where his thoughts and motivations lie.³⁴

Today, intelligence collection against terrorist groups is a particular challenge for intelligence agencies. It is inherently difficult to collect information against a cellular terrorist organization, since the cellular structure was adopted specifically to foil intelligence efforts. Terrorist groups such as Al Qaeda are not nation-states, but are clandestine organizations that are often broken down into small cells of highly dedicated individuals who will not betray their cause.³⁵ Their practice is to keep information about their most lethal plots confined within a small, tightly controlled group of true believers. Such targets are not impossible to locate and deal with, but the task is extremely difficult.

Most terrorists have only partial knowledge of an operation; only “the brain” of the operation knows all the pieces of the puzzle. The capture and interrogation of a terrorist suspect thus provides only a fragment of the whole picture, which must be fused with other scraps of information to reveal a plot. The recruitment of human sources from terrorist organizations is difficult. There is a lack of individuals that can be re-

³¹ Greg Miller, “Emergency Rule in Pakistan; Pakistan’s Nuclear Arsenal a U.S. Worry,” *Los Angeles Times* (8 November 2007): A10.

³² David Batty, “Ricin Discovery ‘No Cause for Alarm’,” *The Guardian* (8 January 2003); available at www.guardian.co.uk/society/2003/jan/08/alqaida.disasterresponse.

³³ Prof. John Le Beau, seminar on “Intelligence Challenges for Democratic States,” November 2007.

³⁴ *Ibid.*

³⁵ Rohan Gunaratna, “The Terror Market: Networks and Enforcements in the West,” *Harvard International Review* (Winter 2006); available at <http://www.harvardir.org/articles/1507/>.

cruited, and most of them are motivated by ideology or religion instead of by material or political considerations, and therefore are very difficult to “flip.”³⁶

Does this mean that intelligence agencies should conduct more technical operations? Are they a more useful approach against these new types of threats? Information that is openly available suggests that Al Qaeda stopped using telephones and other technical modes of communication sometime after the battle of Tora Bora in Afghanistan in late 2001, making it difficult to effectively employ technical types of intelligence collection against the group.³⁷ Anthony H. Cordesman suggests that countries such as Iran that are sophisticated enough to develop nuclear weapons are definitely sophisticated enough to understand the strengths and limitations of modern intelligence sensors, the timing and duration of satellite coverage, and the methods used to track imports and technology transfers. He has written that such groups have learned to cover and conceal, deceive, and create smaller and better-disseminated activities.³⁸ Data on phenomena such as key imports and technology transfers are very important for intelligence collection on proliferation, but those data usually represent only a small fraction of the actual effort. Also, the information collected is often vague and uncertain, “in part because importers and smugglers have every incentive to lie and are familiar with ways to defeat intelligence collection and import controls.”³⁹

Human sources collection frequently is divided between “liaison reporting,” which comes from cooperative foreign intelligence services, and “unilateral reporting,” which is received from agents run by Western intelligence agencies.⁴⁰ Only the integration of all technical and human sources of intelligence can increase our understanding of, and our actions against, international terrorism. George Tenet stated to Congress that “it was this combination, this integration, that allowed us years ago to confirm the existence of numerous Al Qaeda facilities and training camps in Afghanistan.”⁴¹

In addition to traditional methodologies, we need an expanded notion of what intelligence is in order to defeat the new enemy. Greater attention should be focused on open sources of intelligence. Crucial information about the mindsets of terrorists and valuable insights into their cultures can be found on the Internet and in foreign newspapers. Sometimes even hidden messages conveying instructions to terrorist cells could be part of everyday, freely available sources of information.⁴²

³⁶ Prof. Nick Pratt, seminar on “International Terrorism and Security Implications for Democratic States,” George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, November 2007.

³⁷ Interview with Prof. John Le Beau, 20 November 2007.

³⁸ Anthony H. Cordesman, *The War After the War: Strategic Lessons of Iraq and Afghanistan* (Washington, D.C.: CSIS Press, 2004), 56.

³⁹ *Ibid.*, 57.

⁴⁰ Interview with Prof. John Le Beau, 20 November 2007.

⁴¹ Tenet, *Written Statement for the Record*, 4–5.

⁴² Prof. John Le Beau, seminar on “Intelligence Challenges for Democratic States,” November 2007.

Analysis

During the Cold War era, generations of analysts in intelligence services in both the East and West were hired and trained for their knowledge and analytical capabilities concerning the member states of the Warsaw Pact or NATO. But that has changed since 9/11. The twenty-first century requires new analytical skills to be developed to deal with the international challenges posed by terrorism and weapons of mass destruction.

The language capabilities that are now regarded as important by the intelligence services reflect this reality. An understanding of Russian and English is not sufficient to address these new targets. Familiarity with Arabic and other Middle Eastern languages, their cultures and politics, and an understanding of the worldview of Islam have also become crucial.⁴³

As Kie C. Fallis has written, analyses of intelligence data were traditionally directed at subjects such as the nation-state, where the existence, leadership, and location of many actors were not hidden, and therefore easier to examine and analyze. Information covered a wide spectrum, and was not too difficult to collect. This is not the case with analyses of terrorist groups. “Since almost all terrorist groups, and certainly their operational cells, function in a closed, clandestine manner, potential sources of accurate information are almost always limited to sensitive intelligence reporting,” one intelligence analyst has written. “As a result, a terrorist analyst must work harder over a longer period of time in an effort to corroborate reporting and build an accurate profile of a group.”⁴⁴

Fallis argues that the next obstacle for quality terrorism analysis is the level of expertise and experience of the analyst. They have to have very broad knowledge of a wide range of topics. To be able to track one terrorist group, it is necessary to have experience with or a good working knowledge of terrorism itself; knowledge of a specific terrorist group; familiarity with the regional and national issues present in the group’s operating area; and an awareness of Islamic history, religion, culture, sects, etc.⁴⁵ It is obvious that one person cannot accumulate all that knowledge. So is the solution to train individual experts who would have expertise in one particular area (such as Islam, etc.), or is that too expensive?

Former CIA Director George Tenet stated that planning for terrorist operations can span several years, and that is a fact that complicates analysis and warning. The reason is that terrorists are not in a hurry to achieve their goals. After the June 1996 bombing of the Khobar Towers in Saudi Arabia—an attack that killed nineteen U.S. servicemen—Osama bin Laden said that the event was the beginning of the war between Muslims and the United States. Soon after that, he issued a religious edict, or *fatwa* (“Declaration of War”), authorizing attacks against Western military targets on the Arabian Peninsula. Later, in November 1996, when he was asked in an interview “why

⁴³ Ibid.

⁴⁴ Fallis, *Statement for the Record*, 3–4.

⁴⁵ Ibid.

his organization had not yet conducted attacks in response to its August *fatwa* statement, Bin Laden replied, ‘If we wanted to carry out small operations, it would have been easy to do so after the statements, but the nature of the battle requires qualitative operations that affect the adversary, which obviously requires good preparation.’⁴⁶

The next challenge for analysts is the material itself. It is too voluminous and broad to be easily assimilated, but it is also fragmentary and of doubtful credibility. Such evidence can only provide a foundation for guesses about possible terrorist activities, and those guesses could be countless, because those fragments could be pieced together in numerous ways.⁴⁷ One necessity for today’s analysis is to “provide both current reporting and deeper understanding. In solving puzzles about the Soviet Union, analysts worked alone or in small groups, as parts of hierarchies. In trying to understand terrorism, analysts need to be part of larger virtual networks, across specialties and agencies. Moving toward a center-based organization will facilitate those networks.”⁴⁸

Covert Actions

Increasingly, some intelligence agencies have been asked to address twenty-first-century intelligence challenges (such as terrorism) with unorthodox means. In addition to intelligence analysis and collection activities such as espionage, some intelligence organizations have been called upon to actively disrupt terrorist organizations and their ongoing operations. Covert actions deal with direct, often violent actions against targets deemed to represent a threat to national interests, without the sponsoring government having to acknowledge that they have launched such actions. A number of covert actions performed by intelligence services—mainly from the U.S., Israel, and Russia—against modern terrorist targets have taken place over the last few years. These include paramilitary activities, renditions, and in some select instances targeted assassinations (against Hamas and Hezbollah figures, and also Chechen terrorists).⁴⁹

Intelligence organizations have been called upon to conduct these activities probably because such actions do not fall under the basic authorizations for law enforcement units or the uniformed military. In 2005, the *Washington Post* reported that, “on Sept. 17, 2001, [U.S. President] Bush signed a classified Presidential Finding that authorized an unprecedented range of covert operations. The overall counterterrorism program included authorization of lethal measures against terrorists and the expenditure of vast funds to coax foreign intelligence services into a new era of cooperation with the CIA.”⁵⁰ Covert actions can also be “denied” by governments that do not wish to admit

⁴⁶ Tenet, *Written Statement for the Record*, 4–5.

⁴⁷ Roundtable with FBI agents, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

⁴⁸ Gregory F. Treverton, *The Next Steps in Reshaping Intelligence*, Rand Occasional Paper 152 (Santa Monica, CA: Rand, 2005), 7–10; available at www.rand.org/pubs/occasional_papers/OP152/index.html.

⁴⁹ Interview with Prof. John Le Beau, 20 November 2007.

⁵⁰ Dana Priest, “Foreign Network at Front of CIA’s Terror Fight,” *Washington Post* (18 November 2005): A01; available at www.informationclearinghouse.info/article11059.htm.

to sponsorship. Normally they are not conducted by uniformed military forces. One very important aspect of covert actions is that, in most countries, intelligence agencies can pursue covert actions only with the authorization of the head of state (called a “Presidential Finding” in the U.S. context, as described above).⁵¹

Rendition. Rendition is an operation in which suspected terrorists are secretly apprehended and transferred to another country without any judicial review.⁵² The process of rendition has complicated U.S. relations with its allies, particularly in Europe, and has arguably blackened America’s image abroad. The *Washington Post* reported that, since 9/11,

The U.S. government has secretly transported dozens of people suspected of links to terrorists to countries other than the United States, bypassing extradition procedures and legal formalities, according to Western diplomats and intelligence sources. The suspects have been taken to countries, including Egypt and Jordan, whose intelligence services have close ties to the CIA and where they can be subjected to interrogation tactics—including torture and threats to families—that are illegal in the United States, the sources said. In some cases, U.S. intelligence agents remain closely involved in the interrogation.⁵³

The main reason for rendition is to avoid interrogating suspects in the United States, because the level of legal protection for those accused of crimes under U.S. law is very strong. On the other hand, top U.S. intelligence officials have argued strongly that renditions have saved lives, through information obtained from interrogations that would have been illegal in the U.S.⁵⁴

Targeted Killing. Counterterrorism scholar Boaz Ganor defines the assassination of key persons as an individual offensive action, consisting of an attack on an individual or a group who are engaged in initiating, directing, preparing, recruiting, training, or aiding in a terrorist attack. The purpose of such actions is to kill—or at least neutralize—the targeted terrorist.⁵⁵ There are two dilemmas that bedevil this issue. The first is a moral dilemma: Does anybody have sufficient right or justification for intentionally taking a human life? The second is an issue of effectiveness: Intelligence agen-

⁵¹ Alfred Cumming, *Covert Action: Legislative Background and Possible Policy Questions*, CRS Report for Congress (Washington, D.C.: Congressional Research Service, updated 11 October 2007); available at www.fas.org/sgp/crs/intel/RL33715.pdf.

⁵² Dana Priest, “Help From France Key in Covert Operations,” *Washington Post* (3 July 2005): A01; available at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/02/AR2005070201361_4.html.

⁵³ Rajiv Chandrasekaran and Peter Finn, “U.S. Behind Secret Transfer of Terror Suspects,” *Washington Post* (11 March 2002): A01; available at www.infowars.com/saved%20pages/Police_state/torture_wapost.htm.

⁵⁴ Prof. John Le Beau, seminar on “Intelligence Challenges for Democratic States,” November 2007.

⁵⁵ Boaz Ganor, *The Counter-Terrorism Puzzle*, The Interdisciplinary Center, Herzliya, The International Policy Institute for Counter-Terrorism (New Brunswick, NJ: Transaction Publishers, 2005), 112.

cies are organizations of bureaucrats, not killers – can they be trusted to competently carry out such a delicate task? Frederick Hits, the former Inspector General of the CIA, was quoted as saying: “This is not what intelligence officers do. They’re not trained for it.”⁵⁶ The moral question is very difficult to answer, but the question of effectiveness brings into play another issue that could be controversial: the beginning of new forms of cooperation between intelligence agencies and uniformed military commando units/foreign agents, or employees who act on its behalf.⁵⁷ How can the possible joint action of an intelligence service and an armed military unit be coordinated? Who exercises oversight? What are the risks?

International Intelligence Cooperation Today

International Intelligence Cooperation Before 9/11

It is important to note that international intelligence cooperation existed before the attacks of September 2001. The CIA’s secret Counterterrorist Intelligence Centers (CTIC) represent one type of early cooperation. As Dana Priest reported in the *Washington Post*,

[t]he first two CTICs were established in the late 1990s to watch and capture Islamic militants traveling from Saudi Arabia, Yemen, Egypt and Chechnya to join the fighting in Bosnia and other parts of the former Yugoslavia, two former intelligence officers said. ... The intelligence centers were modeled on the CIA’s counter-narcotics centers in Latin America and Asia. Faced with corrupt local police and intelligence services, in the 1980s the CIA persuaded the leaders of these countries to let it select individuals for the assignment, pay them and keep them physically separate from their own institutions.⁵⁸

Agency officials knew that the CIA officers would not be able to adequately respond to terrorist threats, and that they needed a much more intimate knowledge of local terrorist groups and their supporters on the ground.⁵⁹ That is the reason why intelligence interagency teams were “led to Moscow, New Delhi, Islamabad, Riyadh and Sana,” according to 1996 testimony given by Philip Wilcox, the United States’ then-Coordinator for Counterterrorism. “We have held consultations with over twenty governments in the past year [1995], and we have met with counterterrorism experts of the European Union and the Group of Eight. ... A Ministerial Conference on Terrorism of the Group of Eight in Ottawa in December, which grew out of the Halifax Summit in June, addressed concrete ways to enhance international cooperation against terrorism

⁵⁶ Barton Gellman, “CIA Weighs ‘Targeted Killing’ Missions,” *Washington Post* (28 October 2001): A01; available at <http://www.washingtonpost.com/ac2/wp-dyn/A63203-2001Oct27?language=printer>.

⁵⁷ *Ibid.*

⁵⁸ Priest, “Foreign Network at Front of CIA’s Terror Fight,” 2.

⁵⁹ Interview with Prof. Nick Pratt, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

on a global level. The International Conference on Counterterrorism at Baguio in the Philippines last month [March 1996], was the first such initiative in Asia.”⁶⁰

Every cooperative interaction, whether bilateral or multilateral, must be framed by rules of engagement. Rules of engagement are an agreement in written form signed by both sides in which parties agree upon all elements of their future cooperation.⁶¹ Good examples of international intelligence cooperation are those arrangements governing rendition and secret prisons, the so-called “black sites” where the CIA is hiding and interrogating the most important Al Qaeda captives in compounds in Eastern Europe, Thailand, Afghanistan, and Cuba (Guantanamo Bay). Such approaches to intelligence collection depend heavily on cooperation among intelligence agencies in a variety of countries, both those where the sites are located and those where individuals are apprehended and transported.⁶²

Bilateral Cooperation

Before 9/11, bilateral cooperation among countries fighting against terrorist targets was much more developed than multilateral cooperation. The smaller the circle of countries involved in a cooperative intelligence effort, the less opportunity exists for leaks of information. Bilateral relationships allow for greater control over how and with whom shared information is disseminated. It is also much easier to develop relations based on mutual confidence with one country than with several. Bilateral counterterrorism cooperation occurs on an *ad hoc* basis most of the time. A formal method of bilateral cooperation is the LEGAT program, where FBI agents serve as liaison officials in U.S. embassies overseas (the CIA has a similar program).⁶³

The United States and Germany have a strong bilateral relationship in counterterrorism cooperation. The German intelligence agency installed a computer terminal in 1997 in the *Bundeskriminalamt* (BKA, or Federal Criminal Police Office) that is directly linked with the U.S. National Criminal Information Center. BKA officers therefore could access U.S. police files on criminal suspects. Over a period of time, this collaboration became the basis for shared efforts against terrorism.⁶⁴

The United Kingdom has traditionally had a close relationship with the U.S. in many areas; in fact, cooperation between the two nations’ intelligence agencies became

⁶⁰ Ambassador Philip C. Wilcox Jr., Coordinator for Counterterrorism, “Combating International Terrorism,” testimony before the House of Representatives, Permanent Select Committee on Intelligence, Washington, D.C. (5 March 1996); available at http://fas.org/irp/congress/1996_hr/h960305w.htm.

⁶¹ Interview with Prof. Nick Pratt, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

⁶² Dana Priest, “CIA Holds Terror Suspects in Secret Prisons,” *Washington Post* (2 November 2005): A01; available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/01/AR2005110101644.html>.

⁶³ Roundtable with FBI agents, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

⁶⁴ Wyn Rees, *Transatlantic Counter-Terrorism Cooperation: The New Imperative* (London: Routledge, Taylor & Francis Group, 2006).

routine as early as the late 1930s. Since 9/11, it has extended to include counterterrorism efforts. Wyn Rees has written that “a working group on Homeland Security was created between the two states, and the focus has been upon sharing best practices in domestic counter-terror preparations, joint training exercises...”⁶⁵

France and Spain started their close cooperation in counterterrorism efforts in 1984 because of the activities of the separatist group ETA (*Euzkadi Ta Askatasuna*), which was trying to create an independent Basque state in Spain that would also include parts of French territory. ETA had carried out numerous terrorist actions in both France and Spain, most notably a long string of bombings. Rees notes that, “in 1992, France and Spain cooperated in a raid on a property in Bayonne that resulted in [the] capture of many of the senior leadership in ETA.”⁶⁶

Intelligence cooperation between Israel and the Palestinians has always been fraught by many problems, but nevertheless it exists. While the Israel Defense Forces (IDF) controlled the West Bank and the Gaza Strip, where most Palestinian-led terrorist attacks originated, they were able to preempt most terrorist actions. But during the implementation of the Oslo Accords, the IDF left the territory of the Palestinian Authority (PA), and in order to avert terrorist attacks on Israeli soil they had to rely more heavily on intelligence. Prior to the establishment of the PA, Israel cooperated with Palestinian intelligence sources by offering them transit permits, benefits, jobs, etc. But Israel’s withdrawal from the autonomous areas destroyed most Palestinians’ motivation to cooperate with Israeli intelligence agencies.⁶⁷

Dana Priest has written that Ali Abdullah Saleh, the President of Yemen, did not have much control over Yemen’s northern border with Saudi Arabia in late 2001. That part of Yemen turned into a haven for extremists and terrorist training camps. George Tenet, director of the CIA at that time, persuaded A. Saleh to work with the CIA. Tenet provided millions of dollars in aid (including helicopters, weapons, and bulletproof vests) in exchange for Yemen’s cooperation. He also brought in U.S. Army Special Forces trainers to help Yemen create an antiterrorism unit. A. Saleh gave approval for the CIA to fly “predator drones armed with Hellfire missiles over the country.” As a result of that particular cooperation, the CIA “killed six Al Qaeda operatives driving in the desert, including Abu Ali al-Harithi, suspected mastermind of the 2000 attack on the USS *Cole*.”⁶⁸

Cooperation between Indonesia and the CIA started with Washington fulfilling the personal requests of Lt. Gen. Abdullah Hendropriyono, the chief of the Indonesian intelligence service. He requested money for a regional intelligence school, and also asked for help getting a relative admitted into a top-rated American university. The result of this cooperation was the arrest of Muhammad Saad Iqbal Madni, who was linked to the failed British shoe bomber Richard Reid. In addition, Hendropriyono al-

⁶⁵ Ibid., 33.

⁶⁶ Ibid., 35.

⁶⁷ Gaynor, *The Counter-Terrorism Puzzle*, 53–55.

⁶⁸ Priest, “Foreign Network at Front of CIA’s Terror Fight.”

lowed renditions from Indonesian soil, which resulted in Madni being flown to Egypt for interrogation.⁶⁹

A “liaison relationship” is a type of bilateral intelligence cooperation. An intelligence agent of one country is seconded to the service of a host country. Such a relationship has to be formal: the agent is “accredited” by the director of one service to the director of the host service by a formal letter. The fact is that the cover of one officer is being sacrificed in order to gain a good relationship with the other side. The liaison officer must be extremely well prepared for the job. He needs to be fluent in the language of the country where he is “accredited.” In addition, the meeting place or safe house where interactions between the seconded agent and the host agency take place must be well chosen in order to protect the identity of both sides.

The personality of the liaison officers on both sides is another important consideration. Sometimes a good relationship comes to an end with a change of liaison officer if the new agent’s personality is not congenial to his or her counterpart. As part of the U.S. relationship with Saudi Arabia, the CIA would brief the Saudi king on a regular basis. The king was completely against female officers being included as part of the intelligence team. After a long discussion, stressing the fact that a certain part of a briefing could be done only by a female agent, the king accepted. For three years, only that officer briefed the king, and when she changed postings that aspect of the cooperative relationship gradually downsized.⁷⁰

Multilateral Cooperation

Wyn Rees has written of global terrorism that “the growing international dimension of the problem has demanded a more coherent multilateral answer: a terrorist attack may involve the deaths of nationals from several countries, the police investigation may require evidence from more than one jurisdiction, and suspects may be extradited from multiple territories.”⁷¹ Thus, multilateral cooperation is an increasingly prevalent feature in the global counterterrorism arena. Multilateral approaches are being developed both through formal institutions (NATO, EU, UN, etc.) and “informal levels” (Alliance Base).

Cooperation within the EU. Intelligence cooperation within the institution of the European Union did not exist before 2000, when defense intelligence cooperation started as part of the development of the European Security and Defense Policy (ESDP). This is a completely new form of intelligence cooperation in Europe, produced with the help of the European intelligence services but performed under the EU umbrella. The Western European Union (WEU) initiated the process during the 1990s, and most of the WEU institutions have become part of today’s institutional organization of the EU. Three of them represent the EU’s intelligence capacity: The EU Satel-

⁶⁹ Ibid.

⁷⁰ Interview with Prof. Nick Pratt, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

⁷¹ Rees, *Transatlantic Counter-terrorism Cooperation*, 35.

lite Center (EUSC), the Intelligence Division of the EU Military Staff (INTDIV), and the EU Situation Center (SITCEN).

The EUSC is considered to be the first true intelligence capability at the European level. It is mainly tasked with imagery surveillance and works as an early warning unit. The INTDIV is the forum in which military intelligence is exchanged and analyzed. EU High Representative Javier Solana has promoted SITCEN as the primary center of the EU's intelligence architecture. It is the place where all information and intelligence come together and are integrated into the all-source intelligence report. This report goes to the primary ESDP decision makers. The analysis department is the core of this unit. It employs seconded national intelligence agents from the U.K., France, Germany, Spain, Italy, Sweden, and the Netherlands. The EU intelligence cycle is focused mainly on imagery intelligence. EU monitors can only partly be seen as true vehicles for the collection of human intelligence.⁷²

Cooperation within NATO. Multilateral intelligence cooperation within NATO is perhaps best described by an extensive passage from the *NATO Handbook*. It states:

The *Intelligence Division* provides day-to-day strategic intelligence support to the Secretary General, the North Atlantic Council/Defence Planning Committee, the Military Committee, and other NATO bodies such as International Military Staff elements, the Political Committee, and WMD Proliferation Center. It relies on the NATO nations and NATO commands for its basic intelligence needs since it has no independent intelligence gathering function or capacity. On the basis of these contributions, it acts as a central coordinating body for the collation, assessment, and dissemination of intelligence within NATO Headquarters and to NATO commands, agencies, organizations and nations. In addition to providing routine staff intelligence support, the Intelligence Division manages and coordinates the production and dissemination of NATO strategic intelligence estimates, intelligence policy documents and basic intelligence documents, as well as the maintenance of selected databases and digital intelligence information services. It also performs strategic warning and crisis management functions and conducts liaison with other NATO and national bodies performing specialized intelligence functions and related activities. In sum, the Intelligence Division, supported by NATO nations and commands, keeps the Alliance's senior bodies continually informed, facilitates the Military Committee's formulation of military advice to political authorities, provides an intelligence foundation for guiding the composition, organization, and operations of NATO forces, and performs a broad range of tasks in support of NATO defence and political functions.⁷³

⁷² Thorsten W. Etzling, research and scientific assistant at the Geneva Graduate Institute of International Studies, *The Democratic Control of Inter-governmental Intelligence Cooperation*, Working Paper No. 165 (Geneva: Centre for the Democratic Control of Armed Forces, May 2006). For further research on intelligence cooperation within the EU see Jess Pilegaard, *The Politics of European Security* (Copenhagen: Danish Institute for International Studies, 2004).

⁷³ *NATO Handbook*, available at www.nato.int/docu/handbook/2001/hb1103.htm.

Alliance Base: An Example of Multilateral Intelligence Cooperation

The existence of the Alliance Base was first revealed by *Washington Post* articles written by Dana Priest (a 2006 Pulitzer Prize winner) in 2005. They indicate that “the CIA has established joint operation centers (Counterterrorist Intelligence Centers, or CTICs) in more than two-dozen countries where U.S. and foreign intelligence officers work side by side to track and capture suspected terrorists and to destroy or penetrate their networks. ... The secret Counterterrorist Intelligence Centers are financed mostly by the agency [CIA], and employ some of the best espionage technology the CIA has to offer, including secure communications gear, computers linked to the CIA’s central databases, and access to highly classified intercepts once shared only with the nation’s closest Western allies.”⁷⁴ CTICs exist in many countries in Europe, Asia, and the Middle East.

As Priest described the Alliance Bases’ functioning, “The initial tip about where an Al Qaeda figure is hiding may come from the CIA, but the actual operation to pick him up is usually organized by one of the joint centers and conducted by a local security service.”⁷⁵ The Alliance Base center is situated in Paris and includes representatives from Great Britain, France, Germany, Canada, Australia, and the United States. This type of cooperation between intelligence agencies from different countries existed previously, but the formation of Alliance Base represents a positive step toward the codification of such cooperation, therefore making it stronger and more efficient. The Alliance Base is not the work of large army formations; rather, it represents a close cooperative effort of U.S. intelligence case officers and foreign operatives, often in *ad hoc* arrangements.

Alliance Base is headed by a French general “assigned to France’s equivalent of the CIA – the General Directorate for External Security (DGSE).”⁷⁶ So far as we know from available public sources, the Alliance Base “is unique in the world because it is multinational and actually plans operations instead of sharing information among countries.”⁷⁷ The center’s working language is French. As Priest described it, “The base selects its cases carefully, chooses a lead country for each operation, and that country’s service runs the operation.”⁷⁸

The Alliance Base is responsible for identifying, tracking, and capturing or killing the vast majority of committed jihadists who have been targeted outside Iraq and Afghanistan since the 9/11 attacks. “The network of centers reflects what has become the CIA’s central and most successful strategy in combating terrorism abroad,” Priest wrote. “Virtually every capture or killing of a suspected terrorist outside Iraq since the September 11, 2001, attacks—more than 3,000 in all—was the result of foreign intelligence services’ work.”⁷⁹

⁷⁴ Priest, “Foreign Network at Front of CIA’s Terror Fight.”

⁷⁵ Ibid.

⁷⁶ Priest, “Help from France Key in Covert Operations.”

⁷⁷ Ibid.

⁷⁸ Ibid.

⁷⁹ Priest, “Foreign Network at Front of CIA’s Terror Fight.”

Case Study One: The Ganczarski Operation. One of the most successful joint operations of intelligence agencies under the rubric of the Alliance Base is known as the Ganczarski Operation. Christian Ganczarski was a German convert to Islam. He “had been radicalized by a Saudi cleric touring European mosques in the early 1990s, studied Islam on a religious scholarship in the Kingdom, traveled to Afghanistan four times, [and] trained in Al Qaeda camps.”⁸⁰

As Dana Priest wrote, “Ganczarski’s cell phone was the last number that a suicide bomber who killed 21 people on the (*Tunisian*) island of Djerba called in April 2002.”⁸¹ Through communications or signals intercepts (SIGINT), the German intelligence service located Ganczarski and he was arrested. But, according to German law, the origin of the information that connected Ganczarski to the Djerba bombing rendered the evidence inadmissible. In other words, the BND did not have the right to observe a German citizen and collect data from that phone call. Ganczarski was released from prison, and the case was closed, upon which Ganczarski flew to Riyadh, Saudi Arabia.⁸²

The BND decided to continue with the case, so they brought the file to the Alliance Base, and a cooperative operation started. The decision was made to prosecute Ganczarski in France, because some of the casualties in the Djerba bombing were French, and under French law the evidence from Ganczarski’s intercepted phone conversation was admissible in the prosecution. The CIA asked for cooperation from the Saudi intelligence service, and they agreed. The Saudi government had put Ganczarski under house arrest for having an expired pilgrim visa, and had given his family one-way tickets back to Germany, with a change of planes in Paris. But on the flight from Riyadh to Paris he was (unbeknownst to him) escorted by an undercover officer sitting behind him, and a senior CIA officer was waiting when he disembarked in Paris. French authorities separated him from his family and took him into custody.⁸³ “The Alliance Base’s role in the operation was noted obliquely on June 11, 2003, by Interior Minister Nicholas Sarkozy,” Dana Priest reported. “Speaking before Parliament, he said, ‘This arrest took place thanks to the perfect collaboration between the services of the great democracies.’”⁸⁴

Case Study Two: “Operation Albrecht” – The Alleged 2007 Bomb Plot in Germany. “Operation Albrecht” was the code name for the largest German police operation in thirty years – one involving hundreds of intelligence and security agents and

⁸⁰ Priest, “Help from France Key in Covert Operations.”

⁸¹ Ibid.

⁸² Interview with Prof. John Le Beau, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

⁸³ Ibid.

⁸⁴ Priest, “Help from France Key in Covert Operations.”

police officers from across Germany's security community.⁸⁵ As was reported in the *New York Times*,

The discovery [in 2006] of a plot to detonate powerful bombs in Germany ... was the result of close cooperation between American and German security officials, with intelligence passing back and forth between the two sides. ... American intelligence was instrumental in first bringing the foiled plot to the attention of German intelligence and law enforcement officials. ... Interceptions of e-mail messages and telephone calls between Germany and both Pakistan and Turkey raised initial red flags. ... But the Americans also wanted to protect their sources, ... which meant that the earliest warnings were vague.⁸⁶

The *Los Angeles Times* reported that a "U.S. intelligence intercept of suspicious communications between Pakistan and Stuttgart ... was the initial break that ultimately led to the arrest ... of three suspected Muslim militants [Fritz Gelowicz, Daniel Martin Schneider, and Adem Yilmaz] accused of plotting massive car-bomb attacks. ... Authorities said the three claimed allegiance to the Islamic Jihad Union, an Uzbek group that broke off from the Islamic Movement of Uzbekistan, an Al Qaeda ally, in 2002."⁸⁷ U.S. authorities passed the lead along to German police, who conducted a painstaking investigation into the three suspects. After nine months of extensive police work, the suspects were arrested and "were charged with plotting to detonate gigantic bombs made with highly concentrated hydrogen peroxide, of which they had managed to procure three-quarters of a ton," Christopher Caldwell reported in the *New York Times*. "Investigators said the group planned to attack 'soft targets' near American military installations, along with the Frankfurt airport."⁸⁸ According to one journalist, "Several security analysts and one diplomat said the top-secret, international counter-intelligence center in Paris known as 'Alliance Base' may have been involved in Operation Albrecht."⁸⁹

Simply judging by the results, "informal" intelligence cooperation is much more effective than its more formal variants. One of the reasons for this is probably the lack of will to pursue deeper cooperation on sensitive issues that is often present among countries within the context of international organizations. They are still concerned that closer cooperation might jeopardize their sovereignty (this is particularly the case within the EU). As Nick Pratt has argued, "It is said that, when issues are discussed

⁸⁵ Louis Charbonneau, "German Ties with CIA Thrive," *Reuters* (21 September 2007); at http://www.saudigazette.com.sa/index.php?option=com_content&task=view&id=37516&Itemid=14.

⁸⁶ Souad Mekhennet and Nicholas Kulish, "Germans Say U.S. Officials Helped to Foil Bombing Plot," *New York Times* (9 September 2007); at www.nytimes.com/2007/09/09/world/europe/09germany.html?_r=1&coref=slogin.

⁸⁷ "Communications Intercept Led to Bomb-Plot Arrests," *Los Angeles Times* (7 September 2007); available at www.tbo.com/news/nationworld/MGBD1CJ4A6F.html.

⁸⁸ Christopher Caldwell, "Germany on Tiptoe over Terror," *New York Times* (9 September 2007); available at www.nytimes.com/2007/09/09/weekinreview/09caldwell.html.

⁸⁹ Charbonneau, "German Ties with CIA Thrive."

between EU members, everyone can read about the discussion in the press.”⁹⁰ There is also an issue of the quality of the relationships between respective countries. Some relationships are good, others less so. Therefore, countries prefer to cooperate more closely with their political and ideological partners, which creates a state of “partial cooperation” within a multilateral organization. All these reasons contribute to making intelligence cooperation within international organizations very difficult to achieve.

International Intelligence Cooperation on a Formal Basis

One example of formal international intelligence cooperation is the U.S. FBI’s experience working with several different foreign intelligence services on a more structured footing. Types of formal cooperation covered by these relationships include the following⁹¹:

- *Legal Attaché Program (LEGAT)*: FBI agents are stationed in overseas embassies.
- *“Raw intelligence” cables*⁹²: Intelligence is collected in the field, and then sent to FBI headquarters (FBIHQ). FBIHQ prepares raw intelligence cables and then sends them to the appropriate foreign government. Before sending the raw intelligence cables, the FBI redacts the data to protect FBI sources and methods.
- *Training*: The FBI assists foreign governments in training officers from their intelligence services. For example, there is a program in which police officers from foreign countries travel to the FBI Academy in Quantico, Virginia, to receive training.
- *Tracking terrorist finances*: The FBI and other United States government agencies have worked with several different foreign governments to track and freeze the finances of terrorist operations. According to E. Anthony Wayne, the U.S. State Department’s Assistant Secretary for Economic and Business Affairs, “Cooperation between Spanish law enforcement authorities and our Federal Bureau of Investigation is now being facilitated on a day-to-day basis through an FBI agent detailed to Madrid from Washington to work closely with our colleagues from Spain on terrorist financing cases.”⁹³ There are three main areas of international cooperation against terrorist financial networks:

⁹⁰ Interview with Prof. Nick Pratt, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, November, 2007.

⁹¹ The following is drawn from a roundtable discussion with FBI agents at the George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany on 20 November 2007.

⁹² “Raw intelligence” is unevaluated intelligence.

⁹³ E. Anthony Wayne, U.S. State Department, Assistant Secretary for Economic and Business Affairs, “International Cooperation Against the Financing of Terrorism,” talk delivered at the Foundation Jose Ortega y Gasset, Madrid, Spain (16 November 2005); available at www.state.gov/e/eeb/rls/rm/2005/57413.htm.

designations of terrorists and their supporters; United Nations sanctions; and technical assistance and training. Wayne stated in November 2005: “Last May, as one step to address this gap, we agreed to exchange training and technical assistance plans with the European Union, and forwarded a list of training we have conducted and programs we plan to conduct through the end of 2005 to the EU counterterrorism coordinator’s office ... but we have heard that EU member governments—some of the best-placed governments to provide this sort of assistance—are reluctant to share the information even with each other.”⁹⁴

- *Interpol*: FBI agents are assigned to Interpol and cooperate with them in everyday operations.
- *Extradition and rendition*: The FBI works with foreign governments to extradite terrorist suspects (the CIA is often responsible for renditions).
- *Extraterritorial cases*: The FBI conducts work overseas in support of domestic-related investigations. According to the statements of FBI agents at a 2007 roundtable discussion at the George C. Marshall Center in Garmisch-Partenkirchen, Germany, since the mid-1980s, the FBI has investigated more than five hundred extraterritorial cases. In addition to the investigation into the September 11 attacks, several other ongoing extraterritorial investigations rank among the FBI’s highest-profile cases, including the investigation into the 1996 bombing of the Khobar Towers in Saudi Arabia, which killed nineteen United States servicemen; the bombings of the U.S. Embassies in Kenya and Tanzania, which killed twelve Americans; and the bombing of the USS *Cole*, which claimed the lives of seventeen U.S. sailors.⁹⁵

Information (Intelligence) Sharing

Intelligence sharing “has been hailed as a preventive for terrorist attacks, a prophylactic for miscommunication, and the pinnacle of preparedness that every intelligence, law enforcement, and homeland security agency in the government should strive to reach.”⁹⁶ A powerful example of the tragic cost of the lack of information sharing was the failure of the CIA and the FBI to cooperate effectively and share information that they had about Al Qaeda and its capabilities in the months before the 11 September 2001 attacks on New York and Washington. That lack of cooperation resulted in an enormous tragedy, since, between the two agencies, they may have had enough intelligence to disrupt the plot.⁹⁷

⁹⁴ Ibid.

⁹⁵ Roundtable discussion with FBI agents, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

⁹⁶ Shane Harris, “Information Sharing: How They Connect the Dots,” *Government Executive* (1 September 2007): 34.

⁹⁷ For an in-depth discussion see Eleanor Hill, “Joint Inquiry Staff Statement” (17 October 2002); available at www.fas.org/irp/congress/2002_hr/101702hill.html.

Intelligence sharing is a highly delicate issue in transatlantic security cooperation. As Wyn Rees notes, “The sensitive nature of the information, the difficulty of obtaining it and its vulnerability to being compromised makes intelligence a precious commodity that states share only with great reluctance.”⁹⁸ Before 9/11, intelligence sharing was based on a traditional concept of bilateralism, but since 9/11 it has started to take on more multilateral aspects, because “a vital ingredient in fighting terrorism is timely and accurate intelligence.”⁹⁹

There are circles of sharing information between intelligence services. United States intelligence services, for example, share some types of information with no one. Then there is information that is shared only with intelligence agencies within the United Kingdom, or with Alliance Base – that is, only with the United States’ closest allies.¹⁰⁰ But one thing is sure: if you do not share information, you can have only marginal success in fighting global terrorism. On the other hand, by sharing information, you can also get burned (a source could be compromised, there could be an intelligence leak, etc.). The question is how to quantitatively weigh these risks, but the answer is that one simply cannot. There is an unwritten rule, which is called “trust.” The only way things as sensitive as intelligence cooperation and intelligence sharing can work is that parties must trust each other.¹⁰¹

The common interest of each side is the main reason for cooperation in the first place; therefore, there is a reasonable belief that parties are going to play by the rules. There are some other rules besides trust when it comes to sharing information. The first rule is that the first information to be shared is “perishable” information – it is time-sensitive, and it must be shared in time to be useful. The second rule is that of following the “tear line,” which means that intelligence agencies share only those pieces of information that could be useful to their partners, but they leave out any information that could harm them or their sources. The third rule is to follow any third-party agreements that may exist between two countries that have agreed to share information; such agreements dictate that information exchanged will not be shared with anybody else. There is also an issue around what is colloquially known in the intelligence field as the “family jewels,” which means the very best intelligence. High-ranking intelligence officers do not want to share their “jewels,” and the common expectation is that they will not do so.¹⁰² The negative side of intelligence cooperation and information

⁹⁸ Rees, *Transatlantic Counter-terrorism Cooperation*, 90.

⁹⁹ Interview with Prof. John Le Beau, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

¹⁰⁰ Interview with Prof. Nick Pratt, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

¹⁰¹ Roundtable discussion with FBI agents, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

¹⁰² Interview with Prof. Nick Pratt, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, November 2007.

sharing is that a significant percentage of the information exchanged could be useless. But the risk has to be accepted, because there is no alternative.¹⁰³

Conclusion

To fight an enemy that uses multiple measures, a government needs the same ability to employ multiple responses. No single security formation (military, police, gendarmerie) possesses that full scope of operational strengths. These capabilities most often rest with intelligence agencies. They can help to “identify those engaged in terrorism at all levels of involvement and reveal their safe havens and sources of recruitment; track down their weapons, channels of supply, and methods of funding terrorism; warn against future attacks, and thus prevent them; manage crisis situations by transmitting the information decision makers require; disrupt terrorist organizations’ communications networks, and more.”¹⁰⁴

I posed a question to a former intelligence officer from the CIA: Is international cooperation among intelligence agencies the best way to fight terrorism? The answer suggested that there was no need for any further discussion. I felt that I could stop my research immediately.

For example, say that you know about the existence of a person that is considered to be one of the most dangerous terrorists in the world, one who has been responsible for the deaths of hundreds of innocent civilians and is very much capable of continuing with his “duty.” But you do not know whether the person is the number-two ranking leader in Hezbollah or an Iranian intelligence officer. You do know that the person is constantly moving and changing locations, and you know that, when in Lebanon, for example, this person’s “safe location” is hidden behind five built-up blocks from one direction, and six blocks from the other. Thus there is no way to accomplish a physical approach or conduct an operation, or even technical surveillance. You know that “familiar face” people control all streets in this area. And you know that, in order to get at this person, you will need help from Jordanian and Israeli intelligence agencies (which you *may* get), as well as from Syrian and Iranian agencies (which you know you are not going to get), and that the Lebanese are afraid of backlash from Hezbollah if they show that they are willing to help.... How can you find this person, or at least prevent him from planning a future attack?

The only plausible answer, of course, is through cooperation. The greatest problem in conducting global counterterrorism intelligence operations today is that one single intelligence agency cannot possibly have access to all the necessary information. More intimate knowledge of a target is necessary, and only the host country’s intelligence service can provide it. It is logical that more transnational targets need more transnational cooperation. That is why I will dare to say that international cooperation of intelligence agencies is the only way to fight transnational terrorist targets.

¹⁰³ Roundtable discussion with FBI agents, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 20 November 2007.

¹⁰⁴ Ganor, *The Counter-Terrorism Puzzle*, 47.

Of course, there are risks associated with cooperation, chief among them the danger that it might lead to the exposure of the intelligence sources working for the cooperating countries' intelligence agencies. That is why countries are sometimes less motivated to share sensitive information. But that is the risk that we have to take, because there is no alternative. (It is also important to note that agencies are not compelled to cooperate when doing so is not in their common interest.) The question is, How can we make cooperation easier? Can we impose some formal consequences for violating the rules of cooperation? Or can we perhaps create an international center for the collection of sensitive information that will be protected from those that would misuse it?

There are no signs that the present international terrorist threats are going to diminish, even in the distant future. They will only gain in lethal importance if terrorists come into possession of WMD. For this potentially more deadly aspect of international terrorism, there should be a more serious response. Intelligence agencies should become more capable of acting quickly upon the receipt of information about a potential attack. The new security environment will demand immediate reactions, and there will be no time for delay. The operational environment is such that there is concern that renditions or targeted killing will continue in the future.

In sum, cooperation among the intelligence agencies of different countries should be both increased in scope and in depth. One area where key improvements could be made is within international organizations, such as the UN, the EU, NATO, OSCE, etc. Such institutions represent a potentially powerful venue for intelligence cooperation, and one that is not sufficiently exploited. International organizations—especially NATO and the EU—have already developed systems that have been proven to be effective in many areas over long spans of time (the EU in economic cooperation, NATO as a collective provider of security). Strengthening already existing structures or forming new ones that would have much stronger mandates in coordinating or even conducting intelligence work would simplify the efforts and increase the effectiveness of the intelligence operations that they perform. The biggest obstacle to that kind of deeper cooperation is the good will of member countries. We can only hope that the seriousness of future threats will eventually change the stubborn approach of nation-states, broaden their conceptions of their national self-interest, and convince them of the importance of collaboration in the area of international intelligence.