

# Counterterrorism and Intelligence Cooperation<sup>1</sup>

**Derek S. Reveron**

Naval War College

*When the Bush administration declared a global war on terrorism (GWOT) after the September 11 attacks, it was criticized for labeling a tactic as the enemy. But evoking the image of a “global war” highlights the transnational nature of the enemy, and the necessity of international cooperation to combat it. Fundamental to this effort is enhancing bilateral and multilateral intelligence-sharing. This paper explores how the globalization of combating terrorism has broadened the intelligence community.*

## **KEYWORDS**

Intelligence, Islamic Militancy, Counterterrorism

## **BIOGRAPHICAL STATEMENT**

Derek S. Reveron is an Associate Professor of National Security Affairs at the Naval War College in Newport, Rhode Island. He received an MA in political science and a Ph.D. in public policy analysis from the University of Illinois at Chicago. He specializes in security cooperation, democratization, political violence, and intelligence. His books include *Inside Defense: Understanding the 21<sup>st</sup> Century Military* (2008, co-editor), *Flashpoints in the War on Terrorism* (2006, co-editor), *America's Viceroy: the Military and U.S. Foreign Policy* (2004, editor), and *Promoting Democracy in the Post-Soviet Region* (2002).

---

<sup>1</sup> The views expressed in this paper are the author's and should not be interpreted as representing any official position of the United States government.

## Introduction

While most public attention has focused on the “strategic surprise” of the September 11 terrorist attacks against the United States, the events of that day have also spurred a critical, though inconspicuous, examination of how the United States collects, analyzes, and disseminates intelligence. Two years after al Qaeda successfully attacked the U.S., the Intelligence Community’s (IC) poor analysis of Iraq’s weapons of mass destruction program underscored the need for intelligence reform. In the first instance, U.S. intelligence underestimated al Qaeda’s capabilities to execute attacks; in the second case, U.S. intelligence (and many other countries’ intelligence services) overestimated Iraq’s weapons of mass destruction programs and poorly assessed Iraq’s intentions.

Coming within just two years of each other, however, the intelligence failures taught the IC two very different lessons. First, the September 11 attacks have been characterized as a failure to “connect the dots.” If only intelligence agencies had shared their data, analysts could have predicted al Qaeda’s attack, and neutralized al Qaeda’s operatives.<sup>2</sup> Setting aside that it was unlikely the dots were specific enough to connect the overall attack plan with individuals’ names and locations within the United States, “connecting the dots” or sharing intelligence is now a national priority. The second lesson, derived from pre-war intelligence on Iraq, offers a contradictory lesson—“collect more dots.” Although there was human intelligence informing conclusions about Iraq’s weapons programs, it was too limited and just plain wrong. While very few studies separate these lessons, their effects have fundamentally changed the U.S. intelligence community—at the agency and community levels.

This is not unprecedented. By one count, since Japan surprised the United States at Pearl Harbor there have been about 40 commissions that have proposed changes to how the country gathers and analyzes intelligence.<sup>3</sup> Since the September 11 attacks, many Congressional, Presidential, and independent reports have recommended major changes to the intelligence community, culminating with the *Intelligence Reform and Terrorism Prevention Act of 2004*. Among many other things, this Act created the Office of the Director of National Intelligence (ODNI) that is designed to oversee U.S. government intelligence activities and transform the 16 separate agencies and bureaus that compose the U.S. intelligence community. A key ODNI priority is improving intelligence

---

<sup>2</sup> Amy Zegart, for example, argues that organizational problems, not individuals, led inevitably to 9-11, and that deficiencies remain. "If ever we would expect to find a catalyst to transform the U.S. Intelligence Community, the worst terrorist attacks should be it." See *The CIA, the FBI and the Origins of 9-11* (Princeton University Press, 2007).

<sup>3</sup> One of the latest results of this is the *Intelligence Reform and Terrorism Prevention Act of 2004*. This Act created the Office of the Director of National Intelligence (ODNI), which was spurred by the September 11 terrorist attacks and the poor analysis of Iraq’s WMD programs.

cooperation within the United States – in other words, to develop new systems and procedures to break down cultural and technical walls that inhibit connecting the dots. This cooperation is primarily focused within the formal intelligence community, e.g., from FBI to CIA, and between the intelligence community and the law enforcement community, e.g. from FBI to NYPD.<sup>4</sup> In 2007, the United States government issued a *National Strategy for Information Sharing*, which notes: “success in preventing future terrorist attacks depends upon our ability to gather, analyze, and share information and intelligence regarding those who want to attack us, the tactics that they use, and the targets that they intend to attack.”<sup>5</sup>

Though domestic information sharing is an important undertaking and represents a better understanding of how to combat terrorism, this approach overlooks two important points. First, states increasingly rely on other states either for their security or the necessary training and equipment to perform security functions. Second, to combat transnational threats effectively, states must share intelligence at the international level. After all, it was the *Hamburg* cell of largely *Saudis* who executed the September 11 terrorist attacks in the *United States*. Terrorists still come from states, plan operations in states, and operate in states. This paper explores the importance of intelligence in combating terrorism, assesses efforts to share intelligence outside national intelligence agencies, and informs discussions to create an international intelligence community to effectively compete with and combat terrorist networks.

## Global War on Terrorism Created an Opportunity

"Nous sommes tous Américains."  
*Le Monde*, September 12, 2001

When the Bush administration declared a global war on terrorism (GWOT) after the September 11 attacks, it was criticized by some for labeling a tactic as the enemy.<sup>6</sup> But evoking the image of a “global war” highlights the transnational nature of the enemy, and the necessity of international cooperation to combat it. Fundamental to this effort is enhancing bilateral and multilateral intelligence-sharing. The globalization of combating

---

<sup>4</sup> Terrorist attacks are local in nature; so it is much smarter for the FBI to be networked to the communities where terrorists organize and plan their operations, than in a centralized building much afar from the battlefield. To connect the FBI to local law enforcement, it created and funds the Joint Terrorism Task Force (JTTF). According to the FBI’s website (FBI.gov), JTTFs “are our nation’s front line on terrorism: small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. When it comes to investigating terrorism, they do it all: chase down leads, gather evidence, make arrests, provide security for special events, conduct training, collect and share intelligence, and respond to threats and incidents at a moment’s notice.”

<sup>5</sup> National Strategy for Information Sharing, October 2007, p. 1.

<sup>6</sup> Derek S. Reveron and Jeffrey Stevenson Murer, *Flashpoints in the War on Terrorism*, (New York: Routledge, 2006).

terrorism has the potential to strengthen states' warning capabilities by uniting a multinational network of intelligence agencies. Through various political, economic, and military means, the United States has assembled a global coalition to confront terrorism.<sup>7</sup> The 2005 U.S. *National Intelligence Strategy* called for the U.S. intelligence community to "establish new and strengthen existing intelligence relationships."<sup>8</sup> Under the auspices of combating terrorism, there are few countries that will not share intelligence with the United States.

There are many ways to share intelligence. One country may collect and analyze in a particular area and share the intelligence in exchange for intelligence in another area. In this case, the United States identifies a foreign intelligence service's comparative advantage. The U.S. may also provide training in return for services rendered by the foreign service, such as translation. Or, a country may grant the United States use of its territory to collect intelligence in exchange for sharing the information. In other cases, the United States may share collection capabilities with a foreign intelligence service that would share the results of the collection. In the best case of operational collaboration, the United States and a foreign service may undertake combined collection operations. Since September 11, the United States has cultivated intelligence relationships with traditional allies like the United Kingdom, and nontraditional partners like Yemen. Intelligence sharing is not only essential in the war on terrorism, but it also provides a non-public way for governments to cooperate with the United States. In an era when being anti-American (or at least anti-Bush Administration/foreign policy) is popular, this is an important way for governments to cooperate with the United States without incurring criticism from their publics, which are often enflamed by U.S. foreign policies.

What is clear from intelligence activities during the last decade is that the United States now depends more on trusted sources of intelligence information from foreign liaison services, law enforcement agencies, and internal security services to identify terrorist threats than it did in the past.<sup>9</sup> As new diplomatic relationships have been forged during the last several years, the definition of "coalition" has changed dramatically. For many governments that lack either the domestic political support or military interoperability standards to use their armed forces alongside American forces, intelligence-sharing is perhaps the easiest non-public way for governments to show a commitment to U.S.-led efforts to combat terrorism.<sup>10</sup>

---

<sup>7</sup> In 2003, the Bush administration claimed that more than 170 nations were participating in the war on terror. While coalition members have withdrawn from Iraq, there still appears to be relatively widespread commitment to solving political conflicts that provide ideological fuel to international terrorism and cooperating to root out terrorist groups within countries' territories. The White House, "Progress Report on the Global War on Terrorism," Sept. 10, 2003, at [www.state.gov](http://www.state.gov).

<sup>8</sup> John Negroponte, *The National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, Office of the Director of National Intelligence, October 2005, p. 15.

<sup>9</sup> Pillar, *Terrorism and U.S. Foreign Policy*, p. 118.

<sup>10</sup> The public perception is that U.S.-French relations are tense over Iraq, but John McLaughlin, the former acting CIA director, described the relationship between the CIA and its French counterparts as "one of the best in the world. What they are willing to contribute is extraordinarily valuable." Quoted in Dana Priest, "Secret Anti-Terrorism Unit Pairs CIA, Europeans," *Washington Post*, Apr. 7, 2005.

## Categories of Intelligence Sharing Relationships

The countries with which the United States shares intelligence fall into three basic categories: (1) *traditional allies* such as Canada, the United Kingdom, Australia, and other NATO members; (2) *new allies* and nontraditional friends cultivated for the war on terror, such as Pakistan, Yemen, and Uzbekistan; and (3) *traditional adversaries* that have forged new ties with the United States through their intelligence services, such as Libya and Syria.<sup>11</sup>

### *Traditional Allies*

The 1947 UK-USA Agreement between the U.S. National Security Agency and the British Government Communications Headquarters—Canada, Australia and New Zealand joined soon afterwards as “second parties,” and Norway, Denmark, West Germany, and Turkey as “third parties”—established “5 Eyes,” a group that permitted the division of effort in sharing signals intelligence (SIGINT). As the Cold War threat gave way to military operations in the Balkans and Southwest Asia in the 1990s, the relationship between the UK and Australia expanded to provide both countries with access to the Secret Internet Protocol Router Network (SIPRNET), the primary secret-level computer network.<sup>12</sup> These allied intelligence relationships have expanded in the war on terror. In one notable success, U.S. and British intelligence officers secretly traveled to Libya in December 2003 and convinced the Libyans to disclose several dozen facilities, to abandon the country’s WMD programs, and to reach out to British intelligence.<sup>13</sup> These actions by the intelligence services paved the way for Libya’s reintegration into the international community.

Law enforcement also has been a common means for the United States to share intelligence with EU countries. Through the 2003 Container Security Initiative (CSI), the U.S. Customs Service has bilateral arrangements with eight EU member states to prevent global containerized cargo from being exploited by terrorists.<sup>14</sup> In early 2004, then-Coordinator for Counterterrorism Ambassador Cofer Black testified to the Senate Foreign Relations Committee that European intelligence and security forces, known for their

---

<sup>11</sup> This section is based on Derek Reveron, “Old Allies, New Friends: Intelligence Sharing in the War on Terror,” *Orbis* (Summer 2006).

<sup>12</sup> Roger N. McDermott, *Countering Global Terrorism: Developing the Antiterrorist Capabilities of the Central Asian Militaries*, Strategic Studies Institute, U.S. Army War College, February 2004, p. 8; and Amy Butler, “U.S. Nearing Agreement to Allow Coalition Partners Access to Classified Data,” *C4I News*, Potomac, Nov. 27, 2003.

<sup>13</sup> Tenet Briefing.

<sup>14</sup> The White House, “U.S.-EU Summit: U.S.-EU Counterterrorism Cooperation,” Fact Sheet, Office of the Press Secretary, June 25, 2003.

effectiveness in monitoring Islamist organizations, have been credited with stopping numerous mass casualty attacks since September 11.<sup>15</sup>

In addition to its European allies, the United States has also maintained long-standing bilateral intelligence relationships through historic defense relationships in the Asia-Pacific theater. Successive combatant commanders of all U.S. forces in the U.S. Pacific Command have praised the support provided for the war on terror by governments in this region, where intelligence-sharing has been unprecedented since September 11. Singapore, Malaysia, Indonesia, and Thailand have thwarted a number of attacks and have detained or arrested 200 members of Jemaah Islamiyah. In the Philippines, U.S. and Filipino forces worked together in 2002 on the island of Basilan to eradicate Abu Sayyaf Group havens through a combination of civil-military operations and improved counterterrorism coordination.<sup>16</sup>

### New Allies

Since the United States is primarily focused on violent Islamist groups, the greater Middle East is naturally the focus of its intelligence-sharing efforts. Even before September 11, Washington had developed especially helpful relationships with several governments in this region and in Southeast Asia, where the local services have “an enormous advantage in collecting intelligence.”<sup>17</sup> In Saudi Arabia, for example, the impetus for increased cooperation was the 1996 Khobar Towers bombing that killed 19 Americans. The FBI sent several hundred personnel to Saudi Arabia to support the investigation of the attack. According to former director Louis Freeh, the FBI “was able to forge an effective working relationship with the Saudi police and Interior Ministry.”<sup>18</sup> The relationship resulted in the assignment to Riyadh of a legal attaché, who painstakingly developed a relationship with the Saudi General Intelligence Service (known as the Mabaheth).

Since additional attacks there in 2003, the kingdom has been even more cooperative in counterterrorism operations, and has embarked on an aggressive campaign against al Qaeda within the kingdom. In late 2005, FBI Director Robert Mueller praised the U.S. relationship with Mabaheth for disrupting terrorist financing. He told a law enforcement audience in Scotland, “Through this partnership, we have access to the bank records, biographical information, travel histories, telephone records, criminal

---

<sup>15</sup> Ambassador Cofer Black, “Statement” U.S. Congress, Senate, Foreign Relations Committee, subcommittee on European Affairs, Mar. 31, 2004.

<sup>16</sup> Adm. Dennis C. Blair, U.S. PACOM Transcript, Journalists Roundtable, Lemhannas, National Resiliency Institute, Jakarta, Indonesia, Nov. 27, 2001; Adm. Thomas Fargo, “Hearing of the Senate Armed Services Committee, Defense Authorization Request for Fiscal Year 2005,” Apr. 1, 2004, and “Statement,” Senate Armed Services Committee, Mar. 13, 2003; and Ambassador Henry Crumpton, “Press Conference: Manila, Philippines, Oct. 22, 2005.

<sup>17</sup> Kevin Scheid, 9/11 Commission Staff Statement #11, Apr. 14, 2004.

<sup>18</sup> Statement of Louis J. Freeh before the Joint Intelligence Committees, Oct. 9, 2002 (“Freeh Statement”), p. 30.

backgrounds, and employment histories of numerous known or suspected terrorists.”<sup>19</sup> This relationship yielded significant gains by neutralizing significant portions of al Qaeda’s fundraising network and freezing hundreds of millions of dollars.

The relationship with Saudi Arabia also emphasizes the challenges of sharing intelligence with new allies with different intelligence practices. According to U.S. Ambassador to Saudi Arabia Robert Jordan, U.S. intelligence had to “work through a cultural tendency not to share intelligence information, not to share the results of investigations until the investigation was fully completed and wrapped up neatly in a bow. Rather than the interactive, full contact kind of intelligence-sharing that American culture is more used to.”<sup>20</sup>

Washington’s relationship with Yemen has also been fruitful. With Yemeni roots, bin Laden had a significant network there and likely considered it a potential post-Afghanistan refuge.<sup>21</sup> Working with Yemen resulted in the arrests of more than one hundred al Qaeda members and a November 2002 CIA missile strike that killed al Qaeda’s top operative in Yemen. Other political and military actions have helped strengthen the government of Yemen to conduct counterterrorism operations. Intelligence activities provide a small U.S. footprint that is tolerable in countries like Yemen where anti-Americanism is high.

Outside the Middle East, intelligence-sharing partners have been instrumental in the roundup of key al Qaeda leaders in South Asia. With Pakistan’s proximity to Afghanistan and its historical support for the Taliban, Pakistani support has been critical in the hunt for al Qaeda in Afghanistan and Pakistan. As a full-fledged partner of the United States, Pakistan has provided an air corridor, bases for logistics, and most importantly, intelligence-sharing. Cooperation with Pakistan has netted the most significant members of al Qaeda to date. Pakistani authorities arrested Abu Zubaidah, a Palestinian member of al Qaeda, in March 2002, and in September 2002, Ramzi Binalshibh, whom then-U.S. Attorney General John Ashcroft named one of the most wanted suspects in the September 11 attacks. And in March 2003, Khalid Sheikh Mohammad, the chief operational planner of the September 11 attacks, was arrested in Rawalpindi, Pakistan. In all three cases, Pakistan intelligence cooperated with the United States and handed the al Qaeda members over to the United States. In 2003, FBI Director Mueller testified to the importance of these arrests: “Our view of the capabilities of Al Qaeda becomes more transparent and it gives us more confidence that we have an

---

<sup>19</sup> Department of State, *Patterns of Global Terrorism 2003*, Apr. 29, 2004; Mueller at NAA.

<sup>20</sup> Robert Jordan, “Crises and Opportunities in U.S.-Saudi Relations,” Interview with Saudi-U.S. Relations Information Service, Sept. 3, 2004.

<sup>21</sup> After 9/11, then-ambassador to Yemen Sanaa Edmund Hull commented, “By some accounts, bin Laden had looked at Yemen as a possible refuge if he were driven out of Afghanistan. So I think it’s very important that we head off problems and resolve problems in Yemen as effectively as possible.” Edmund Hull Interview, “In Search of al Qaeda,” *PBS Frontline*, Oct. 6, 2002, at [www.pbs.org](http://www.pbs.org); “American Killed in CIA’s Attack in Yemen,” *BBC News*, Nov. 7, 2002.

understanding of plots in the past, plots that were on the table, and future possibilities.”<sup>22</sup> As current affairs in Pakistan reveal, the nation is essential to bringing stability to Afghanistan and confronting al Qaeda.

### **Non-Traditional Allies**

The final category of intelligence-sharing relationships includes non-traditional partners and state sponsors of terrorism. Shortly after September 11, Yang Youming, ministerial counselor of the Embassy of China in Washington, stated, “Since terrorism now crosses borders, it has become everyone’s problem. All countries need to be willing to work together by sharing intelligence.” Indeed, Washington now praises China’s intelligence-sharing and diplomatic backing for the war on terror, and plans to station an FBI officer in Beijing.<sup>23</sup> The two countries’ signing of the CSI in July 2003 established a new antiterrorism relationship between Chinese Customs and the U.S. Department of Homeland Security. Intelligence cooperation will be needed to meet the goal of CSI: identifying and checking high-risk shipping containers before they are delivered to the United States.

In addition to China, the United States has opened a dialogue with several countries that are on the State Department’s list of state sponsors of terrorism. Libya, Sudan, and Syria have provided terrorist-related intelligence since September 11. In this context, the United States finds itself in partnership with rogue states that have changed their view on international terrorism. In 2003, Libyan leader Moammar Qaddafi pronounced Islamism “a threat to all regimes in the region” and began work with the United States that ultimately led to the shutting down of Pakistani scientist A. Q. Khan’s nuclear proliferation network. Because Sudan was the primary home of Osama bin Laden in the early 1990s, that country has been critical to providing intelligence on al Qaeda. Though Iran was included in President Bush’s “axis of evil” in 2002, as early as 1998, Iranian intelligence used well-established channels of communication to warn Western intelligence agencies of a dangerous alliance growing between the Taliban and bin Laden. And despite frosty relations between the two nations, there have been cases of information-sharing between the Iranian Ministry of Intelligence and National Security and U.S. intelligence agencies through Jordanian intelligence. Finally, Syria has become one of the CIA’s most effective and prolific sources of intelligence allies in the fight against al Qaeda, and has provided hundreds of files on al Qaeda cells throughout the

---

<sup>22</sup> Robert Mueller, Director of the FBI, “Hearing of the Commerce, Justice, State and Judiciary Subcommittee of the Senate Appropriations Committee,” Apr. 10, 2003.

<sup>23</sup> Panel Discussion, “Counter-Terrorism Strategies in the Post 9-11 Era: International Cooperation (What Works and What Doesn’t),” Potomac Institute for Policy Studies, Nov. 26, 2001, comments by Yang Youming; Ann Tyson, “U.S., China Cautiously Rekindle Military Ties,” *Christian Science Monitor*, Feb. 20, 2002.

Middle East and in Muslim communities in Europe.<sup>24</sup> For example, Syria gave the U.S. valuable intelligence on al Qaeda that helped thwart an al Qaeda attack on the U.S. Fifth Fleet headquarters in Bahrain and an attack on an American target in Ottawa.<sup>25</sup>

While these new relationships with non-traditional allies are hopeful, larger political disputes with the governments of Iran and Syria threaten to undermine progress made at the operational level in combating terrorism. Ongoing international concern for Iran's nuclear program and Syria's involvement in Lebanon, coupled with these countries' support for their own terrorist groups, make these new relationships tenuous at best. While U.S. operations in Iraq have exacerbated these relationships, an optimistic assessment identifies intelligence-sharing as the basis for normalizing relationships.

## Dissemination not Discrimination

The United States *National Intelligence Strategy* establishes three core objectives for developing these intelligence relationships. First, “engage and invigorate friendly foreign intelligence services’ efforts that could aid in the identification and disruption of terrorist organizations abroad and within U.S. borders.” This requires high levels of trust on the part of all countries involved and increased acceptance of U.S. intelligence operating on another government’s territory. Second, “coordinate closely with foreign intelligence services to inform a common assessment of threats and options in response.” With coalition warfare the norm in U.S. foreign policy, the United States recognizes the importance of allied governments’ operating from a common intelligence picture—global issues require global consensus. Finally, “ensure that insights gained from our foreign intelligence relationships inform intelligence judgments and develop effective options in response.” Just as the U.S. intelligence community depends ever more on open-source information in intelligence assessments, so too does it expect to derive additional value from foreign government information. While the benefits to expanding the network of intelligence agencies are obvious, it is difficult to overcome suspicion and traditional statist practices that eschew sharing.

The September 11 Commission’s conclusions for intelligence-sharing within the U.S. intelligence community are as true for intelligence-sharing with foreign liaison services: “Current security requirements nurture overclassification and excessive compartmentalization of information among agencies. Each agency’s incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few

---

<sup>24</sup> Jane’s Terrorism Watch Report Daily Update, Jan. 13, 2003, at [www4.janes.com](http://www4.janes.com); Michael Hurley, “Statement,” U.S. Congress, National Commission on Terrorist Attacks Against the United States, Washington, D.C., Staff Statement #5, Mar. 23, 2004; Mahan Abedin, “The Iranian Intelligence Services and the War on Terror,” *Terrorism Monitor*, May 20, 2004; Seymour Hersh, “Annals of National Security, The Syrian Bet,” *New Yorker*, July 28, 2003.

<sup>25</sup> Seymour Hersh, “The Syrian Bet,” *The New Yorker*, July 28, 2003; and William James Martin, “Clean Break with the Road Map,” *Counterpunch*, February 14/15, 2004: 12-14.

rewards for sharing information.”<sup>26</sup> The first (and now former) Undersecretary of Defense for Intelligence Stephen Cambone recognized this problem within the Defense Department and issued a memo to defense intelligence agencies that stated, “Incorrect use of the NOFORN [U.S.-only consumers] caveat on DoD information has impeded the sharing of classified national defense information with allies and coalition partners.” Cambone subsequently prescribed new means to ensure the widest dissemination of intelligence information and demanded “intelligence under the purview of the DoD, originators shall use the ‘Releasable to’ (REL TO) marking, and any subsequently approved releasability marking to the *maximum extent possible*.”<sup>27</sup> U.S. military officers serving with non-American forces now insist that the only valuable intelligence is that which can be shared with coalition partners. With so many coalition partners in Afghanistan, and to a lesser extent Iraq, sharing intelligence with dozens of U.S. partners ranging from Mongolia to Georgia is vital to operations. In 2007, the Bush Administration offered an approach to codify these practices when it released a *National Strategy for Information Sharing* that outlined five principles to guide intelligence-sharing.<sup>28</sup>

With some foreign intelligence services, regular meetings may be sufficient to share information. In other cases, common training, classification criteria, standardized security clearance procedures, and compatible intelligence systems are necessary components to cultivating cooperation. To overcome challenges and facilitate information exchange across a diverse group of allies, the United States developed a new information-sharing architecture called Combined Enterprise Information Exchange System (CENTRIXS).<sup>29</sup> The system not only enables the United States to collaborate with its partners, but also allows the partners to collaborate with one another.

The level of trust, value of intelligence, and type of diplomatic relationships with other countries determine the extent to which intelligence is shared. But penetrating another country’s intelligence service remains a threat: in February 2001, the FBI arrested Special Agent Robert Hanssen for spying on behalf of Russia. And in 2005, there were several counterintelligence cases that involved some of America’s closest allies, including the Philippines and Israel. As the United States develops intelligence relationships with foreign intelligence services, counterintelligence concerns will increase. The threat of espionage remains, but cooperation is the imperative guiding counterterrorism efforts. The challenge is to mitigate counterintelligence threats while enhancing counterterrorism operations.

---

<sup>26</sup> Pillar, *Terrorism and U.S. Foreign Policy*, p. 186; Cronin and Ludes, *Attacking Terrorism*, p. 85; and 9/11 Commission Report, p. 417.

<sup>27</sup> Stephen A. Cambone, “Memorandum: Use of the “Not Releasable to Foreign Nationals” (NOFORN) Caveat on Department of Defense (DoD) Information,” May 17, 2005. Emphasis mine.

<sup>28</sup> *National Strategy for Information Sharing*, p. 26.

<sup>29</sup> Anteon International Corporation developed CENTRIXS based on the LOCE system used within NATO. See “What We Offer/Functional Solutions/Homeland Security” at [www.anteon.com](http://www.anteon.com).

## Pitfalls of Sharing: Lessons from Iraq WMD Assessments

The new emphasis on intelligence-sharing creates new challenges, including how to widely disseminate classified information, overcome sensitivities regarding intelligence sources and methods, and maintain counterintelligence vigilance. Even with regard to combating international terrorism, national interests still govern states' behaviors. And when expanding beyond traditional allies, a variety of practical and counterintelligence concerns arise. The fear of introducing fabricated intelligence is best exemplified by the 2002 *National Intelligence Estimate* on Iraq's weapons of mass destruction programs.<sup>30</sup>

Practically all information about Iraq's alleged biological weapons programs came from a single human source (an Iraqi chemical engineer) code-named "Curveball." In 2000 a foreign liaison service brought Curveball to the attention of the U.S. intelligence community which did not gain direct access to the source until May 2004, a year after the Iraq war began. But between January 2000 and September 2001, the Defense Intelligence Agency disseminated almost 100 foreign intelligence reports from Curveball regarding mobile biological weapons facilities in Iraq, which formed the basis for Secretary of State Colin Powell's 2003 presentation to the UN Security Council. While subsequent investigations determined that Iraq had no new plans for biological weapons after 1996 and that Curveball had fabricated the information he provided to the foreign service, this episode exposed serious shortcomings in intelligence tradecraft – particularly verification of the source's bona fides – and the dangers of relying on a foreign service for intelligence.<sup>31</sup>

Additionally, there are countries that have a wealth of information to share about terrorists, but with whom relations create problems for U.S. foreign policy. Some countries, like Uzbekistan, are opposed to the American democratization project; others,

---

<sup>30</sup> In addition to the discussion on Iraq's biological weapons below, the Iraq case provides many examples of relying on foreign intelligence. For example, Czech intelligence insisted that September 11 hijacker Mohammed Atta met with Iraqi intelligence in Prague. While the FBI and CIA could not verify this claim and the 9/11 Commission provided evidence that Atta was in the United States during the alleged meeting, the Bush administration used the Czech intelligence report as a key piece of "evidence" linking Iraq to Al Qaeda. See the *9/11 Commission Report*, p. 228. And in the most infamous case to illustrate the pitfalls of sharing foreign intelligence, one need only consider the statement made by President Bush in the 2003 state of the union address. "The British government has learned that Saddam Hussein recently sought significant quantities of uranium from Africa." The statement based on British intelligence was not only wrong, but the claim sparked an investigation leading to the indictment of Vice President Cheney's chief of staff, Lewis ("Scooter") Libby. For an excellent treatment of the origins of British intelligence on Iraq, see John Cassidy, "The David Kelly Affair," *New Yorker* Dec. 8, 2003, [http://www.newyorker.com/fact/content?031208fa\\_fact2](http://www.newyorker.com/fact/content?031208fa_fact2)

<sup>31</sup> The Duelfer Report does make clear that serious doubts about the source's credibility existed prior to Secretary Powell's presentation, but those doubts were not communicated to Powell. See CIA, *Comprehensive Report of the Special Advisor to the Director of Central Intelligence on Iraq's Weapons of Mass Destruction*, vol. III: Biological Weapons, Sept. 30, 2004, pp. 83–86. Ultimately, the Iraqi Survey Group "found no direct evidence that Iraq, after 1996, had plans for a new BW program or was conducting BW-specific work for military purposes." *Ibid.*, p. 1.

such as Syria, more directly sponsor terrorist groups to promote their national interests. Relationships such as these can also create tensions within the U.S. bureaucracy, as evidenced by a disconnect between the departments of State and Defense over Uzbekistan's human rights record. While the Defense Department was paying the Uzbek government for use of a military base, the State Department was trying to sanction that same government for human rights violations. The current counterterrorism strategy, however, requires the cooperation of all interested states, no matter how distasteful they may be to the United States. The challenge is to extract useful information from these foreign intelligence services without becoming tainted by their tactics or supporting techniques inconsistent with universal human rights practices.<sup>32</sup> As combating terrorism increasingly becomes a war of ideas, relationships with unsavory foreign intelligence services create challenges for U.S. strategic communication efforts, which are trying to improve America's image abroad.

## Improving Analytical Processes

While sharing may be a virtue in international politics today, it is essential that sharing produces results. At a minimum, a re-conceptualized international intelligence community should be able to improve intelligence analysis through three distinct activities. First, parse all-source intelligence in order to determine as many of the available, credible pieces of information (henceforth "dots") as possible. Second, separate the credible information from all the irrelevant data (wheat from chaff). Finally, organize and connect the credible "dots" to produce a sound analytical judgment. These three things are essential elements of good intelligence analysis, but there are significant challenges.

When it comes to information sharing, there is a "secrecy versus efficiency dilemma." Many of the "dots" of relevant information are part of sensitive operations/investigations and are jealously guarded by the responsible agency/government. While it makes sense to subject data to the widest possible group of analysts, there are genuine operational security concerns that must be met. All intelligence services owe it to their sources to protect their identities. This has given rise to the debate about "need to know" versus "need to share."

A more mundane challenge to intelligence sharing is transliteration and naming conventions. Until better naming algorithms are used to capture the many ways to transliterate names from one alphabet to another, there is a fundamental communication problem.

A more serious concern is how different services understand the "enemy." As more countries share intelligence analysis, it is important for analysts and policymakers

---

<sup>32</sup> Cronin and Ludes, *Attacking Terrorism*, p. 130; Lawrence Freedman, ed., *Superterrorism: Policy Responses* (Cambridge: Blackwell Publishing, 2002), p. 159.

to understand national biases. This is critically important with opposition groups that are labeled “terrorist” for political expediency.

## **Beyond a World of Suspicion**

The maxim, “the enemy of my enemy is my friend,” has guided countries to share intelligence throughout history. Today, the shared enemy is transnational and preys on weak states and provokes the response of developed states. Terrorism, human trafficking, and drug smuggling are central concerns of both strong and weak states. Intervention lessons of the last decade underscore the importance of non-traditional intelligence support to post-conflict reconstruction efforts. Political exploitation of ethnicity, organized crime, political corruption, and at-large war criminals undermine international efforts of state building. For American and coalition forces to be successful in peacekeeping, peace enforcement, and counterterrorism, a new approach to intelligence is required. For the international community to be successful, intelligence must not only shift from the strategic-level to the street-level, but also from U.S. ONLY to U.N. RELEASABLE. To move beyond a world of suspicion is unreasonable (and maybe unhealthy), but mutual trust, compatible systems, and common laws and policies are required.