OPEN SOURCE INFORMATION
The Missing Dimension of Intelligence

A Report of the
CSIS Transnational Threats Project

Authors
Arnaud de Borchgrave
Thomas Sanderson
John MacGaffin

March 2006
About CSIS

The Center for Strategic and International Studies (CSIS) seeks to advance global security and prosperity in an era of economic and political transformation by providing strategic insights and practical policy solutions to decisionmakers. CSIS serves as a strategic planning partner for the government by conducting research and analysis and developing policy initiatives that look into the future and anticipate change. Our more than 25 programs are organized around three themes:

Defense and Security Policy—With one of the most comprehensive programs on U.S. defense policy and international security, CSIS proposes reforms to U.S. defense organization, defense policy, and the defense industrial and technology base. Other CSIS programs offer solutions to the challenges of proliferation, transnational terrorism, homeland security, and post-conflict reconstruction.

Global Challenges—With programs on demographics and population, energy security, global health, technology, and the international financial and economic system, CSIS addresses the new drivers of risk and opportunity on the world stage.

Regional Transformation—CSIS is the only institution of its kind with resident experts studying the transformation of all of the world’s major geographic regions. CSIS specialists seek to anticipate changes in key countries and regions—from Africa to Asia, from Europe to Latin America, and from the Middle East to North America.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is a bipartisan, nonprofit organization headquartered in Washington, D.C., with more than 220 full-time staff and a large network of affiliated experts. Former U.S. senator Sam Nunn became chairman of the CSIS Board of Trustees in 1999, and John J. Hamre has led CSIS as its president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2006 by the Center for Strategic and International Studies. All rights reserved.

Library of Congress Cataloging-in-Publication Data
CIP information available on request
ISBN-10  0-89206-483-8

Cover image: © Images.com/CORBIS

The CSIS Press
Center for Strategic and International Studies
1800 K Street, N.W., Washington, D.C. 20006
Tel: (202) 775-3119
Fax: (202) 775-3199
E-mail: books@csis.org
Web: www.csis.org/
Contents

Project Participants  iv
Foreword  v
Acknowledgments  viii
Authors’ Note: Recent U.S. Government Efforts on OSI  ix

Introduction  1

Intelligence and Counterterrorism: Today’s Landscape  2

So, What’s Out There in the World of OSI?  3

A Growing Awareness of the Importance of OSI  12

CSIS’s Approach to Acquiring and Exploiting OSI with the Help of a
Trusted Information Network  14

The Second Year—What Do We Propose?  21

Conclusion  22

Appendix: Potential Areas of Investigation for the CSIS Trusted
Information Network  24

About the Authors  26
Project Participants

**Authors**
Arnaud de Borchgrave  
*CSIS*

Thomas Sanderson  
*CSIS*

John MacGaffin  
*CSIS*

**Core Advisory Group**
Timothy J. Galpin  
*Johns Hopkins Applied Physics Laboratory*

Aimee Ibrahim David  
*DFI International*

David Kay  
*Consultant*

John MacGaffin  
*CSIS*

Richard P. O’Neill  
*The Highlands Group, Inc.*

Suzanne E. Spaulding  
*Bingham Consulting*

Jonathan Winer  
*Alston & Bird*

**Project Coordinator**
Jacqueline Harned  
*CSIS*

The opinions, conclusions, and recommendations expressed or implied in this report are not necessarily the product of a Core Advisory Group consensus, nor do they necessarily represent the views of their organizations.
Foreword

The United States and its allies are struggling in the War on Terrorism. Tactical successes dot the landscape since September 11, 2001, but the larger strategic battle is in serious jeopardy. Neither the global politico-religious ideological struggle nor its terrorist manifestations can be grasped solely with top secret intelligence reports. This global counterterrorism campaign cannot succeed without the adequate exploitation of open source information and nongovernmental expertise. A longstanding bias for classified information within the intelligence community and among its many customers constitutes a serious obstacle to these international counterterrorism efforts. Terrorist tactics, organization, and motivations are not intuitive to most people trying to prevent such attacks. These aspects of terrorism, however, are the province of hundreds of experts from around the globe. This makes the ongoing terror threat one that requires increased “outside” help if we are to address it effectively.

This “outside” expertise includes people like Sydney Jones of the International Crisis Group. Jones understands both the smallest details and the wider strategic significance of the terror threat in Southeast Asia to a degree envied by Western intelligence services. Another is the Germany-based journalist Mark Hibbs, who, while writing for obscure nuclear energy trade journals over the last two decades, revealed much of the nuclear arms proliferation network run by Pakistan’s A.Q. Khan. This information, if matched with disparate pieces of classified intelligence, could have shed significantly more light on the secret efforts to obtain nuclear weapons by North Korea, Libya, and Iran. Unfortunately many of these experts are most often consulted on a one-off basis, rather than as core, central participants in the intelligence process.

Clues to the source of potential future attacks in the United Kingdom could have been found by reading Le Canard Enchaine, the traditional French repository for government leaks by unhappy functionaries. Only weeks before the July 7, 2005, London bombings, this publication printed a leaked, classified report written in June 2005. The report, by France’s domestic intelligence service Renseignements Generaux (RG), noted that close surveillance of the Pakistani community in the United Kingdom was now critical to avoid a major incident. The French weekly quoted the 20-page RG report as saying that attacks “will be carried out by agents who will take advantage of the pro-jihad sympathies within the large Pakistani community in the U.K.”

The 2005 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, or the “Robb/Silberman Report,” highlighted intelligence and policy failures leading up to the war in Iraq. The report also noted the failure to develop intelligence on a range of first-tier threats such as terrorism and proliferation. With regard to the current campaign against terrorism, the Robb/Silberman Report stated “open source information provides a base for understanding classified materials. Perhaps the most important example
today relates to terrorism, where open source information can fill gaps and create links that allow analysts to better understand fragmented intelligence, rumored terrorist plans, possible means of attack, and potential targets.”

More than 170 individuals inside and outside of governments across Europe, North Africa, the Middle East, and North America were interviewed for phase I of this study. A framing conference in Oslo, Norway, helped shape this feedback into the open source study. A subsequent workshop in Brussels helped design and then “test” the open source, trusted information network model. Findings were vetted throughout the study by a seven-member core advisory group and several experts from around the globe. Phase I of the CSIS study found, among other points:

- Government counterterrorism and intelligence collection methods cannot be properly applied without the understanding and calibration that open source information and nongovernmental expertise can provide. Open source information, broadly construed, will be at least as important in the world’s counterterror efforts as secret intelligence was during the Cold War.

- There remains a failure to recognize that the new, unbounded forces of international terrorism represent a different threat environment, one that requires a major focus on open source collection to complement the rare but highly valuable insight derived from covert collection.

- U.S. military, intelligence, and law enforcement agencies remain seriously challenged by terrorism. The fact remains that in the four and one-half years since September 11, these agencies have been, in essence, the primary forces arrayed by the United States against terrorism and have been operating with only a partial understanding of the problem they face.

- The effort to engage open source, nongovernmental expertise across borders is not meant to supply actionable intelligence that identifies a particular terrorist on a certain street, but instead to share information and knowledge about the terrorist and his/her environment.

- Many in the intelligence community are well aware of the value of open source information and the universe of experts outside of the classified world, but there is no comprehensive program to exploit this talent. Outside experts are most often engaged and consulted on a one-off basis, rather than as core, central participants in the intelligence process.

- Unlike during the Cold War, much of the value added information or “intelligence” on today’s threat resides in foreign language databases and in foreign minds. The United States does not have reliable access to either.

Future, large-scale terrorist attacks against the United States are likely. They will be perpetrated by individuals and groups that have significant advantages over the intelligence, police, and other government forces charged with

---

preventing the next attack. The intelligence gap highlighted in the Robb/Silberman Report can be reduced with a well-planned, thorough, and committed effort to exploit open source information and by engaging trusted networks of nongovernmental experts. Enhanced tools and approaches must be brought to bear on a threat that has rendered Cold War–era intelligence capabilities and thinking inadequate. Expertise and data found in the public realm across numerous countries, individuals, and information sources will be a critical factor in the ongoing counterterror campaign.

Judge William H. Webster  
*Project Chair*

Arnaud de Borchgrave  
Thomas Sanderson  
*Project Principal Investigators*
Acknowledgments

The authors gratefully acknowledge the contributions made by the project’s Core Advisory Group, which helped make this project a success. That group includes the Johns Hopkins Applied Physics Laboratory, DFI International, the Highlands Group, Inc., Bingham Consulting, and Alston & Bird. Additional acknowledgment is given to John MacGaffin, a CSIS senior adviser who provided valuable guidance and direction throughout the life of the project and who also coauthored this report.

CSIS would like to thank Alain Wouters, founder, Whole Systems Inc., for moderating the Brussels conference and Maurice Sonnenberg, senior international adviser, Bear Stearns & Co., Inc., who provided guidance to the project’s principal investigators.

CSIS would also like to thank the more than 100 current and former national intelligence directors, security service chiefs, diplomats, military, and judicial officials from the United States, Europe, and North Africa who were interviewed for this project; as well as the more than 50 academic, private-sector, and other nongovernmental specialists from several nations who contributed their time and knowledge and participated in the Oslo and Brussels conferences. We are grateful for their candid discussions and their unique insight into the pressing issue of multilateral information and intelligence sharing on counterterrorism. Additional thanks goes to Forsvarets Forskningsinstitutt (FFI), the Norwegian Defense Research Establishment for providing assistance in conducting the Oslo conference, and Espace Moselle for hosting the Brussels conference.

This project was made possible by the generous financial support of the Smith Richardson Foundation and the Norwegian Foreign Ministry. Overall support for the Transnational Threats Project is provided by the Sarah Scaife Foundation without whose contribution our work could not be accomplished. The staff of the Transnational Threats Project, most notably Jacqueline Harned, assistant director, as well as Deborah Stroman, Mike Brizendine, Saltanat Berdieeva, Katja Gersak, Eduardo Serra, and Molly Krause, played key roles in research and project management.

The opinions, conclusions, and recommendations expressed or implied in this report are not necessarily the product of a project participant consensus nor do they necessarily reflect the official views of our project sponsors.
Authors’ Note
Recent U.S. Government Efforts on OSI

In a timeframe almost identical to the period in which the research and preparation of this report were carried out, the U.S. intelligence community, under the leadership of the new director national intelligence (DNI), John Negroponte, came to its own conclusions about the importance of open source information to the nation’s overall intelligence effort. To transfer that into government reality, the DNI has mandated two important steps. First, the new position of assistant deputy director of national intelligence for open source (ADDNI/OS) was established within the office of the DNI, and at the CIA, the 65-year-old Foreign Broadcast Information Service (FBIS) has been designated as the core of the new Open Source Center, which will serve the open source needs of all 15 members of the intelligence community, as well as other government departments and agencies.

Eliot A. Jardines is the ADDNI/OS and is responsible for developing strategic direction, establishing policy and managing fiscal resources for open source exploitation under the DNI. The head of the FBIS, Douglas J. Naquin, is now head of the Open Source Center.

The findings of this study provide clear support for the concerns that motivated the DNI to take the steps described above. More important, the focus on trusted information networks, which this study advocates and now advances as the central focus of phase II, points the way to a dimension of open source information acquisition and exploitation that remains, at least for the time being, beyond the reach of the traditional intelligence services. As this report will demonstrate, the addition of the expertise that resides in the multiple members of a trusted information network will provide a critical complement to the focus on new, robust databases, new analytic tools, and communications channels that the DNI-mandated enhancements will be able to bring to the table. In short, this is an exciting example of mutually reinforcing work being done in parallel inside and outside the intelligence community.
Open Source Information
The Missing Dimension of Intelligence

Arnaud de Borchgrave, Thomas Sanderson, and John MacGaffin

I used to think when I worked in the intelligence service that the government was always saying “go and get us a pail of water on the subject of terrorism. We’re thirsty, we want to drink.” And I would look outside my office and only see mist.—CSIS Terrorist Threat Information Sharing Project Participant, October 2004

Introduction
The global counterterrorism campaign cannot be successful without the adequate exploitation of open source information. A long-standing bias for classified information within the intelligence community and among its many customers may constitute a serious obstacle to international counterterrorism efforts. Over the course of one year, CSIS conducted research, traveled extensively for interviews, and convened two major conferences in Europe—all of which helped to confirm and further define the seriousness of this problem. CSIS has now organized a unique effort that, in conjunction with our international partners and others, will develop and then turn over to governments and outside experts alike a working model for significantly enhanced information sharing on counterterrorism, which has open source information (OSI) and a trusted information network (TIN) of individuals at its core.

The following report shares some of what we learned in the course of phase I of the project and discusses the way ahead in this new and potentially critical area of information sharing and open source exploitation. We believe that important perspectives on the shape and pace of terrorism in Europe are already beginning to emerge through this prism of unclassified information. When the expertise

1 The specific focus of the CSIS study was on the threat posed by European-based terrorists who have fought in the Iraq insurgency and are returning with enhanced capabilities.
available to our TIN is brought to bear in the next year, we believe that even
greater understanding of the terrorist threat in Europe will be developed. Most
importantly, when this is ultimately combined with the privileged and sometimes
more focused classified information obtained by numerous cooperating
governments, we will have created an important new tool to assist us all in our
efforts to combat terrorism.

We welcome the comments, as well as the ongoing involvement, of those who
share our vision of the importance of this aspect of international counterterrorism
efforts.

**Intelligence and Counterterrorism: Today’s Landscape**

The United States employs almost 100,000 people in 15 intelligence agencies at a
cost of $44 billion each year. Among the European members of NATO, about the
same number work for over 100 intelligence and security services.

The practice of secrecy, a crucial aspect of successful professional intelligence
operations common to agencies worldwide, has led to a general reluctance to
share classified information. And this, in turn, leads to the abuse of the “top
secret” rubber stamp. In the United States, a record 15.6 million documents were
classified in 2004, double the number in 2001, at a cost of $7.2 billion, according
to the federal Information Security Oversight Office. Documents are classified at
the rate of 125 a minute, or 180,000 a day. Many consist of information from
open sources that then become secret.

Meanwhile, declassification has throttled back from 204 million pages in 1997
to 28 million pages in 2004. There are numerous indications that the environment
of secrecy has unintentionally prevented the production of sound intelligence. The
chairman of the 9/11 Commission, Thomas Kean, a former Republican governor
of New Jersey, said the failure to prevent Al Qaeda’s 2001 attacks stemmed not
from leaks of sensitive information, but from barriers erected to prevent the
sharing of information between government agencies and the public.

Analysts tend to give more weight to a folder stamped “Secret” than to the
latest public broadcast of an Al Qaeda message on the Al Jazeera satellite
television network. Could this, perhaps in part, explain why the extent of the
radicalization of Muslim youth in Western Europe appears to have caught U.S
and European intelligence and policy communities by surprise? Nongovernment
experts working entirely from open source material, by contrast, seem to have
been focused on this issue for some time and had been writing in great detail
about what was happening inside Europe’s Muslim communities.2

---

2 For a superb article on Muslim integration in Europe, see Robert Leiken, “Europe’s Angry
Muslims,” *Foreign Affairs* 84, no. 4 (July/August 2005).
So, What’s Out There in the World of OSI?

Informed by transatlantic discussions on this subject over the past year, CSIS compiled an informal “sampler” of those key aspects of terrorism on which OSI, independent of other input, is able to make important contributions. This inventory merely touches the surface of what could be available and is presented here as a quick, interesting, and illustrative survey of the OSI universe relative to terrorism.

What Can OSI Tell Us about Al Qaeda and the Internet?

Drawing solely on a broad range of open source information, CSIS first warned about “cyberterrorism” in a report published in 1998, entitled Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo. Long before 9/11, Al Qaeda used the Internet, along with other forms of communication, to plan and execute its 1998 attacks on U.S. embassies in Kenya and Tanzania and the bombing of the USS Cole in Aden harbor in 2000. Today, there are significant parts of a “virtual caliphate” in cyberspace. Some 4,000-plus pro–Al Qaeda Web sites, chat rooms, and message boards diseminate propaganda, broadcast news, recruit new adherents, and praise successful jihad while denigrating the infidel. The ready availability of sizeable numbers of computer engineers and scientists at the service of transnational terrorism also enables this cyber caliphate to add to its tool kit the ability to send instructions to followers using seemingly innocous coded messages or more advanced, state-of-the-art encryption techniques.

Most of these 4,000 Web sites emerged after September 11, 2001, and together they constitute the communications backbone of a violent Islamist movement. This world of online jihad is not something imaginary, theoretical, or conceptual—it exists. Its many visionaries, participants, and supporters all work toward the day when the removal of secular Arab leaders of traditional Muslim lands transforms the virtual caliphate into a political-religious reality.

In his book Smart Mobs,3 the Internet visionary Howard Rheingold says mobile phones will soon metamorphose into tiny multimedia terminals, the kind of disruptive technology that changes important aspects of national security, including counterintelligence and counterterrorism on the “good guy’s side” and, on the “bad guys’ side,” the means of carrying out terrorism and espionage. Before long, electronics will be worn, implanted, or ingested. The appliances we carry in our pockets or wear in our clothing will become supercomputers that talk to each other through a wireless mega-Internet. The new era, beginning in 2010, could transform most intelligence collection to open source information. This will also enable “people to act together in new ways and in situations where collective action was not possible before,” said Rheingold.4 Al Qaeda’s computer-literate terrorist geeks were among the first to get there.

---

4 Ibid., p. xvii.
Untraceable e-mails can inform, organize, and encourage terrorists across continents. Islamist extremist recruits use the Internet not only to follow the philosophic debates that rage from Kandahar to Cairo to Chicago, but also to learn how to make bombs from household chemicals; to learn the names of martyred fundamentalists, as well as the locations of mosques in Syria and Jordan that can hide and protect a militant on his way into Iraq; and to learn different locations in Iraq where Islamist extremists should report for training and combat assignments. The well-organized riots and protests in January and February 2006 against the Danish cartoon depictions of the Prophet Muhammad are a good demonstration of this online ability to organize violence worldwide.

**What Can OSI Tell Us about Islamist Extremist Ideology and Motivation?**

Many intelligence analysts are puzzled by Osama bin Laden’s growing popularity in the Muslim world. They cite the “Muslim mainstream” as the likely counterforce that ultimately will defeat the “Islamist extremist fringe.” But, except for an occasional quiet effort at criticizing this extremist ideology, there has been no such moderate Muslim outcry even though more than four years have elapsed since 9/11. This continues to be the case despite numerous extremist outrages, with many of the victims themselves Muslim.

Why is this so? Recall that it was not long ago when millions of Europeans living in Western democracies pledged allegiance to Joseph Stalin, history’s most murderous dictator with the blood of some 40 million victims on his hands. Between the end of World War II in 1945 and Stalin’s death in 1953, Communist parties in France and Italy, blindly loyal to the Kremlin, consistently garnered 25 percent of the electoral vote. In 1948, the Italian Communist party would have won the elections and taken over the government if the United States had not covertly bankrolled anti-Communist parties.

After World War I, the inaugural conference of the Communist International set out to communize the entire world, and this effort continued until the eventual demise of the Soviet Union 70 years later. In the 1930s, before World War II, large numbers of Europeans, embittered by the fallout of the Great Depression and the apparent weakness of their democratic leaders, succumbed to the totalitarian temptation of left and right. Stalin, Hitler, and Mussolini enjoyed fanatical followers throughout Europe. Today, bin Laden and “Islamofascism” are experiencing the same surge in popularity. The moderate Muslim mainstream is likely to succumb to these temptations, as did many in the European mainstream 85 years ago.

Al Qaeda recruits its extremists in many of the same spawning grounds used by Communist parties during the Cold War. Disenfranchised, often disrespected, and frequently unemployed, Muslim youth living in the poorer Muslim neighborhoods of major European cities are easily influenced by propaganda depicting the United States and Israel as being on a crusade against Islam. It is important to note that many European Muslims residing in the middle class are
also experiencing the frustration, marginalization, and disrespect of their poorer brethren.

In *Globalized Islam: The Search for a New Ummah*, Olivier Roy, one of France’s leading scholars of modern Islamism [and an indispensable fount of open source intelligence], notes striking parallels between today’s jihadists and Europe’s radical left of the 1960s and 1970s. The two movements have drawn from similar social pools of alienated, dislocated youth. They have chosen similar symbols (beards and guns and sanctified texts: the Koran substituting for Marx, Sayed Qutb, the Egyptian whose theories inspired the Muslim Brotherhood, for Gramsci) and targets (“imperialism,” “globalization,” “Americanization”). The jihadists’ notion of a pan-Islamic *Ummah*, or nation, says Roy, recalls the Trotskyists’ idea of the proletariat: “an imaginary and therefore silent community that gives legitimacy to the small groups pretending to speak in its name.” The triumph of Islam is held to be, as the triumph of socialism once was, “inevitable.” 5,6

Jonathan Randal, in his book *Osama: The Making of a Terrorist*,7 gives substance to even deeper echoes by relating the testimony of a captured Al Qaeda convert. Kemal Daoudi, “the son of Algerian immigrants to France, was a brilliant engineering student. But when poverty forced his family to move to a grim Paris suburb, he awoke suddenly to what he called the abominable treatment meted out to all the potential ‘myselfs’ who had been conditioned to become sub-citizens, good only to keep working to pay for the retirements of the ‘real’ French when the French age pyramid gets thin at the base.”8

The choices he, and countless thousands of similar children of immigrants, felt they faced were either to fall into depression or, as Daoudi did, “to react by taking part in the universal struggle against this overwhelming iniquitous cynicism.” Daoudi went off to Afghanistan, became a committed extremist, and returned to Paris, where he was detained as part of a plot to blow up the U.S. embassy.9

**What Can OSI Tell Us about the War for Muslim Minds?**

The research of Rona Fields at George Washington University emphasizes the middle- or upper-middle-class backgrounds of 75 percent of known anti-Western terrorists, the majority of whom have some college education. Some analysts infer from these statistics that the ghettoization of the less fortunate coreligionists was not the catalyst that drew them to Al Qaeda. Others argue it was precisely this factor that persuaded them only violence would alter the status quo, in much the

---

8 As quoted in Rodenbeck, “The Truth about Jihad.”
9 Ibid.
same way that the Cold War’s Red Brigades in Italy, Red Army Faction and Baader-Meinhof Gang in Germany, and France’s Action Directe thought that it was only through violence that they could collapse “bourgeois” societies.

Gilles Kepel, arguably France’s best known authority on political Islam, points out in his latest book, *The War for Muslim Minds,* yet another resemblance between radical leftists and Islamist extremists, this one created by erroneous outside perceptions that could have been avoided by taking OSI seriously. Samuel Huntington’s *The Clash of Civilizations*... and other texts, says Kepel, facilitated a subtle “transfer” of the West’s Cold War strategic outlook: “The parallel drawn between the dangers of communism and those of radical Islam gave Washington’s strategic planners the illusion that they…could simply transpose the conceptual tools designed to apprehend one threat to the very different realities of the other…. [They] were culturally incapable of grasping an actor that was not, in the final analysis, a state…. The strategy of destroying the Taliban and then annihilating Saddam Hussein’s ‘rogue state’ presented the advantage of being operational: it allowed the Pentagon to use its panoply of high-tech weapons, forged in the confrontation with the USSR…but it missed the intended target. The very intangibility of the Al Qaeda network precluded a traditional military conquest.”

While it is certainly too early in our investigations to make such a statement with any certainty, the foregoing discussion begins to raise the question of whether the United States and other Western governments’ focus on the classified insights to terrorist activities obtained by their intelligence services has led them to that most egregious of all traps into which a policymaker can fall—underestimating the enemy. Did we and our international partners fail to adequately credit open source indicators prior to 9/11? Certainly. Do we and they still fall into that trap? It increasingly appears to be that way.

In “The Truth about Jihad,” Max Rodenbeck suggested that the intelligence community had been unable to deliver a simple understanding of who and what the United States was up against. Was it just Osama bin Laden and his Al Qaeda organization, and if so, what made this man tick? What attracted people to his ideas? How best to defuse their potency? Was the danger “terror” in general or rather a particular strain of Muslim fundamentalism? Or was it perhaps some flaw in the Middle Eastern body politic that rendered that whole region a breeding ground for hostility to the United States?

The answers to these questions have grown clearer over time. And most of the clarity has come from more focused use of information available in open sources and, importantly, from the interaction and iterations of experts such as those who constitute the CSIS Trusted Information Network. As a result, something of a

---

consensus seems to be emerging about the causes, effects, and best means of dealing with violent Islamist radicalism.

What Can OSI Tell Us about Europe's Islamist Extremists?
The Iraq War and subsequent occupation energized Islamist extremists. The conflict and ensuing unrest provided a practical training ground for more lethal and sophisticated terrorists who will haunt the West, as well as the Middle East, for decades to come. Islamist extremists from Europe's increasingly marginalized Muslim communities began leaving for Iraq to fight Americans shortly after the collapse of the Hussein regime. Scores—some say hundreds—have now returned home, carrying with them newly acquired urban combat skills. This scenario was widely predicted in 2003 by diplomats, generals, and academics in open sources, but decisionmakers claimed they were not briefed on this dangerous development.

The back-to-back London bombings in July 2005, perpetrated by homegrown terrorists and utilizing store-bought bomb components, could not have come as a surprise to those who had read or heard the inflammatory pro–Al Qaeda proselytizing of extremist imams that covered London and its environs every day. Protected against deportation by British passports, their Friday prayers were tantamount to an incitement to violent action, also protected by freedom of speech and tolerated under the guise of multiculturalism.

For years, British authorities failed to understand that readiness to accommodate was not seen as a sign of strength by the radicals. They look on tolerant inclusive instincts as signs of Western decadence that make a society rudderless and deserving of cultural conquest by an emergent caliphate. Omar Bakri Mohammed, the extremist Muslim preacher who routinely promoted violent struggle, lionized the July 7 bombers as “the fantastic four,” praised the 9/11 terrorists, called British troops in Iraq “terrorists,” and said he would not inform the police if he became aware of Muslims planning a terrorist attack. He then flew to Lebanon for a vacation, and London announced he would not be allowed back. Ten others were also ordered to be deported. Britain’s long tradition of sheltering foreign radicals, from Karl Marx to Islamist firebrands, is protected by laws the government sought to repeal before being blocked by Parliament.

Lord John Stevens, a former chief of London’s Metropolitan Police, estimates the number of Al Qaeda supporters in the United Kingdom at between 10,000 and 15,000. Polls in the London Daily Telegraph and other UK newspapers on the opinions of Britain’s Muslims are chilling: 25 percent say Muslims should not inform on people linked to terrorist activities; 38 percent have suffered abuse because of their religion; 80 percent agree the “Bush-Blair war on terror” is a war against Islam; 42 percent feel British society does not respect Muslims; 22 percent see a “serious contradiction between being a good British citizen and Islamic values”; 53 percent feel they do not belong to Britain.

If only 1 percent of Europe’s 20 million Muslims are seduced by the Islamist extremist siren call, those 200,000 represent a formidable potential army who believe their duty is to fight Christian and Jewish oppressors. Add to that 1
percent of the remaining 1.3 billion Muslims elsewhere in the world, and the numbers do begin to appear daunting.

U.S. history is also a major focus of discontent by Islamic and other radicals across Europe. The litany of issues—beginning with the United States’ Founding Fathers as slave owners, followed by the institution of slavery, the internment of Japanese-Americans in World War II, the fire-bombing of Tokyo, and the atomic bombs dropped on Hiroshima and Nagasaki—are easily blended into a seamless picture designed to inspire loathing for the United States’ cultural heritage. British academics who track the proselytizing of extremist clerics and their influence over Muslim youth saw the explosion coming, as did French academics who saw nationwide Muslim riots in the making.

One British citizen of Indian descent, who was arrested in the London terrorist attacks, was also wanted in the United States where authorities accused him of conspiring to set up a terrorist training camp in Oregon for Islamist extremists to “fight jihad in Afghanistan.”

Belatedly, the British government introduced tough new laws on the expulsion of hate mongers to their countries of origin, but they were rejected by the House of Commons. Prime Minister Tony Blair has proposed that any new citizen “actively engaged” with Web sites, bookshops, networks, and organizations judged to be inciting hatred be deported, while naturalized citizens or dual nationals be stripped of their citizenship and also open to deportation. Mosques implicated in inciting violent action would be shut down. However, not all of these provisions were accepted by the British Parliament.

France’s Renseignements Generaux (RG), an intelligence service that monitors domestic trends, reported shortly before the London bombings that close surveillance of the Pakistani community in Britain was now critical to avoid a major incident. Written in late June 2005, the 20-page report said the United Kingdom “remains threatened by plans decided at the highest level of Al Qaeda.” The attacks, said the RG, “will be carried out by agents who will take advantage of the pro-jihad sympathies within the large Pakistani community in the U.K.”

Despite this, following the May 2005 general election, Britain’s Joint Terrorism Analysis Centre (JTAC), which receives input from MI6, MI5, New Scotland Yard, and other intelligence and law enforcement bodies, lowered the threat level from “severe” to “substantial” one month before the attacks. Three of the four bombers who carried out the July 7 attacks that killed 56 people were Britons of Pakistani origin.

Across the channel, France does not hesitate to close mosques that have become centers of extremist agitation and expel their imams back to North Africa. The French government concluded, long before its EU partners, that lax immigration procedures, such as Britain’s, imply that host countries do not expect...
loyalty from naturalized foreigners and give incoming Muslims the idea that Western countries have no self-respect.

Yet the French chose to ignore the unmistakable warning signs of a major upheaval that OSI provided. In 1995, the French movie *Hate* showed the burning cars of 2005, whose message was a denunciation of police brutality. Actually, the police no longer dared patrol after dark in a “hot” suburb like St. Denis on the outskirts of Paris.

Rap music and movies have reflected the grinding poverty and mood of France’s immigrant underclass. Disturbing new slogans were hurled in the recent French riots: Paris became Baghdad-on-the-Seine; “This is Jerusalem”; and the beginning of Europe’s “intifada.” Many Muslims in their 30s and 40s were involved; it was not exclusively the “spontaneous teenage” stereotype.

About one-fifth of Germany’s 2,500 main mosques are under the sway of Milli Gurus, an offshoot of a party banned in Turkey, which claims 87,000 members across Europe (including 50,000 in Germany) and distributes literature urging resistance against “the oppressing imperialist designs.”

No intelligence analysis on Spain’s Muslim extremists would be complete without the kind of open source texture provided by Yale University’s Maria Rosa Menocal, author of *Ornament of the World*.15 Madrid is ever mindful that one of Europe’s strongest intellectual and cultural forces centered on tenth-century al-Andalus (Arabic for the Iberian Peninsula) and its capital city of Cordoba, which, at its peak, was light-years ahead of any contemporary European society. Muslim control of al-Andalus lasted 800 years, ending in 1492 with the surrender of the last Muslim stronghold in Granada.

**What Can OSI Tell Us about the Nuclear Wal-Mart?**

By the end of 2003, if not before, the United States had all the information it needed to confront President Pervez Musharraf with irrefutable evidence of leakage of Pakistan’s nuclear secrets to nations hostile to the United States—Iran, North Korea, and Libya. U.S. intelligence agencies had painstakingly connected all the dots of Pakistan’s secret “nuclear Wal-Mart,” run by the father of Pakistan’s nuclear arsenal, A.Q. Khan, for the benefit of the United States’ enemies. An early indication of the existence of this nuclear bazaar surfaced in the classifieds of a Pakistani newspaper 10 years before. It listed secret nuclear weapons ingredients that were for sale. The advertisement was the work of an overzealous executive on Khan’s team and was quickly pulled before drawing the attention of the intelligence community. One Western intelligence officer caught it and reported it to headquarters as a hoax. An open source–based, trusted information network with a focus on nuclear proliferation may have taken the information more seriously.

---

An Iranian publication recently carried an advertisement that called for applications from aspiring “martyrdom seekers.” Men and women were urged to enlist with the “Lovers of Martyrdom Garrison.” Those selected were to be given “specific and specialized training.” The objective was “to achieve all-round readiness against the enemies of Islam and the sacred Islamic Republic and to protect the foundations of Islam.”

The publication is produced by an institute run by one of Iran’s most conservative and radical clerics, Ayatollah Mazbah Yazdi, reportedly spiritual adviser to Iran’s new president, Mahmoud Ahmedinejad. In a speech delivered before the presidential election and broadcast on Iranian television, Ahmedinejad said, “Is there art that is more beautiful, more divine and more eternal than the art of martyrdom? A nation with martyrdom knows no captivity.”

If chosen after submitting their curricula vitae to PO Box 16535-664, Tehran, suicide volunteers were to be given a choice of three targets: “occupiers of the Islamic holy sites” (referring to U.S.-occupied Najaf, Karbala, and other places in Iraq); “occupiers of Jerusalem” (referring to Israel); and Salman Rushdie, the author of Satanic Verses, against whom the late Ayatollah Khomeini issued a fatwa sentence of death in 1989. (This despite the fact that the fatwa was subsequently annulled by Iran’s mullahs.) Hamas, Hizballah, and Islamic Jihad have also extolled martyrdom and publicly solicited suicide bombers against Israel. Sri Lanka’s Tamil Tigers (LTTE) organization, is the world leader in suicide bombing.

Open source material on twenty-first-century kamikazes is abundant. University of Chicago professor Robert Pape, who authored Dying to Win, has done watershed work on the psychology of the suicide bomber across many cultures. Although Pape seems to ascribe nationalist sentiment as the primary motivation of most suicide bombers, there is also an extensive body of evidence taken from failed bombers, which shows that they, at least, thought that God, not government, wanted them to do this. But whatever the truth, there are significant sources of OSI available on this subject. And surely, a profound understanding of what motivates suicide bombers is an essential element in developing an effective, integrated plan to combat them. Yet Western governments and intelligence services—relying on their classified sources of information and, perhaps, on preconceived assessments and desired outcomes—seem not to have arrived at the same conclusions.

What Can OSI Tell Us about the Proliferation of Radical Ideologies?

Harvard Business School professor John Quelch says the arrest of an Egyptian chemistry Ph.D., who studied at the Universities of Leeds and North Carolina, in

---

connection with the July 7, 2005, bombings in London highlights the potential vulnerability of academic institutions to terrorist organizers.\(^{18}\)

An indiscriminating tolerance of diversity of opinion, even of extremist rhetoric, says Quelch, provides an excellent arena for those seeking to condition impressionable young minds in classrooms, in campus meetings, or in student societies. What might be termed dangerous behavior in the “real world” is excused in academia as eccentric and benign, even necessary.

NATO Supreme Commander General James L. Jones, who as head of the U.S. European Command (EUCOM) has responsibility for most of sub-Saharan Africa, is concerned with the proliferation of Al Qaeda–type cells in Niger, Mali, and Mauritania. Training in counterinsurgency was subsequently extended in that region. But plans soon went awry in Mauritania. A no-nonsense, pro-American president, Ould Sid Ahmed Taya, ran Mauritania, one of only three Arab League nations to recognize Israel, as a benevolent strongman. He had ordered the imprisonment of known Islamist extremist activists and sympathetic soldiers and politicians—but not for long. A colonel promoted himself to president while Taya was next door in Niger, appointed a new prime minister, and ordered the Islamist extremists released.

The impact on European society of the “Arab boomer” generation will be dramatic and massive. It will find a permanent place on the menu of an open source, trusted information network. Michael Vlahos of the Joint Warfare Analysis Department at Johns Hopkins University’s Applied Physics Laboratory did not need secret information to see that the “bow wave of the Arab boomer generation, buoyed by aggressive illegal immigration, is pushing the proportion of Muslims in France, Italy and Spain, up to 25 percent or even one-third of their population. Working adults may reach 40 percent or more. And the period from 2010 to 2050 could even alter the very nature of European civilization.”\(^{19}\)

Bernard Lewis, a leading scholar of Islam, believes Europe will have Muslim majorities in the population by the end of the twenty-first century. What seems certain today is that the European model of a welfare state is unsustainable, which could lead to the disintegration of the European Union.

In 1900, one out of four human beings on the planet lived in Europe. Today it is 10 percent. In 20 years time, the baby dearth, coupled with longer life spans, will bring it down to 7 percent. With the average European woman bearing 1.8 children—the replacement rate is 2.1 children—Europeans will be 1 in 14 in the world. The world population is growing by the equivalent of one new Mexico—nearly 100 million people—every year. And most of this growth is in countries that can barely supply essential services.

One immediate fallout from the demographic projections was on television screens the world over during the riots that rocked the North and West African


suburbs of major French cities. These were the second and third generations of Muslim parents, who had come to France to take the menial jobs native French were no longer willing to do. While it did not trigger the upheaval, Islamist fanaticism and secret Al Qaeda cells certainly played a major role in stoking the fires throughout France in October and November of 2005.

The Palestinian uprising that began in 1987 with stones and gasoline bombs evolved into a suicidal terrorist war by the late 1990s. Some observers of Islam in Europe believe this process may be beginning, not just in France, but also in the rest of Europe.

A Growing Awareness of the Importance of OSI

CSIS is not, of course, the only OSI voice in the wilderness. Increasingly, various government and quasi-government studies have concluded that in order to properly focus traditional secret intelligence efforts against the terrorist threat, we must first acquire a much greater understanding of those aspects of the problem that the terrorist does not directly control, but which necessarily shape his environment and his actions. This contextual knowledge can help make sense of other, disparate pieces of intelligence. For this reason, we have come to refer to OSI as the “missing dimension” in counterterrorism intelligence.

Throughout the course of our project, a number of U.S. government commissions reported their findings on September 11 intelligence failures, as well as on shortcomings in the intelligence assessments of Iraq’s weapons of mass destruction capabilities. The various commission results emphasize the need to increase the use of both open source information and nongovernmental experts with specialized knowledge directly and indirectly related to terrorism and other threats facing the United States and its allies.

Specifically, the National Commission on Terrorist Attacks Upon the United States, commonly referred to as the 9/11 Commission, found that, among other things, “the importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to ‘connect the dots.’ No one component holds all of the relevant information.” As many proponents of open source information lament, the term “all-source intelligence” has often overlooked OSI as a vital component of what constitutes a comprehensive, “all-source” package. Or, put another way, OSI constitutes one (or more) of the dots that were missing in the past and, unless a new course is set, will certainly be missing in the future.

A second investigation into intelligence and policy failures, undertaken by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, whose findings are commonly referred to as the Robb/Silberman Report or the WMD Report, placed tremendous emphasis on

Arnaud de Borchgrave, Thomas Sanderson, and John MacGaffin

OSI.\textsuperscript{21} This emphasis was not focused exclusively on failures in assessing the capabilities of a state such as Iraq, but on the United States’ ability to develop intelligence on a range of first-tier threats such as terrorism and proliferation. The Robb/Silberman Report noted the following with regard to OSI and outside expertise:

Open source information provides a base for understanding classified materials. \textit{Perhaps the most important example today relates to terrorism}, where open source information can fill gaps and create links that allow analysts to better understand fragmented intelligence, rumored terrorist plans, possible means of attack, and potential targets.\textsuperscript{22} (Emphasis added.)

This is particularly important now that Al Qaeda and scores of other terrorist groups have transitioned from training at actual camps in Afghanistan to widespread and sophisticated Internet-based training. This virtual training camp network is invisible to policymakers and to many in the intelligence community, but it is all too real, highly effective, and difficult to monitor and stop. As the Robb/Silberman Report goes on to say about clandestine collection challenges:

\begin{quote}
[M]any open source materials may provide the critical and perhaps only window into activities that threaten the United States…. Regrettably, the Intelligence Community’s open source programs have not expanded commensurate with either the increase in available information or with the growing importance of open source data to today’s problems. This is an unacceptable state of affairs.\textsuperscript{23}
\end{quote}

Finally, the \textit{Intelligence Reform and Terrorism Prevention Act of 2004} requires that

\begin{quote}
…the DNI [director of national intelligence] shall ensure that the intelligence community makes efficient and effective use of open source information and analysis. It is the sense of Congress that the DNI should establish an intelligence center for the purpose of coordinating the collection, analysis, production and dissemination of open source intelligence….\textsuperscript{24}
\end{quote}

The exact way in which this recommendation will be implemented is still under review, but there is widespread agreement throughout government that it is on the mark.

While CSIS’s efforts in this project are focused on the role that OSI and TINs can play in countering terrorism, it is clear that many other transnational threats could be better understood with greater use of the same outreach and network tools. Former deputy director for intelligence John Gannon stated it well in testimony to Congress:

\begin{quote}
\textsuperscript{22} Ibid., pp. 378–379.
\textsuperscript{23} Ibid., p. 378.
\end{quote}
Clandestinely derived intelligence is as valuable as ever, but, in my recent experience, open source information now dominates the universe of the intelligence analyst, a fact that is unlikely to change for the foreseeable future. Open source information today is indispensable to the production of authoritative intelligence community analysis. It increasingly contains the best information to answer some of the most important questions posed to the intelligence community. By contrast with the Cold War period, the center of gravity for expertise…is outside of the intelligence community.  

Gannon’s remarks highlight the gap between the analysts’ need for greater access to OSI and the problems of providing that access in a community that developed in a “secret-centric” world. Our report constitutes an important step in highlighting this discrepancy and suggesting possible ways forward.

CSIS’s Approach to Acquiring and Exploiting OSI with the Help of a Trusted Information Network

Many facets of terrorism can best be understood by those academic, social, criminal, political, religious, and cultural disciplines infrequently considered by intelligence community analysts. This makes terrorism a threat that requires “outside” help if we are to address it effectively. A government analyst making full use of OSI, and linked to a trusted information network with multinational expertise, will have a much better understanding of the terror threat, and be better positioned to prepare responses to it, than the analyst whose major information inputs largely favor classified intelligence. Understanding that an intelligence analyst is overwhelmed by the massive amount of OSI, CSIS’s trusted network of individuals can contribute significantly to analysis by its very operation. Network members will not only access highly relevant open source information, but through their dynamic interaction can provide the kinds of unexploited or altogether new insights so desperately needed to counter terrorism.

Thus, against this backdrop CSIS is exploring how best to bring that open source information and multiple sources of international expertise to bear on those terrorists planning once again to attack Europe and the United States. The result of the year-long phase I study is, we believe, a rigorous exploration of the problem and a thoughtful map to improve understanding and analysis of terror threats. Phase II is bringing a “real-world test bed” to our findings and theories. And at the end of the test bed, we hope to be able to offer our government partners, fellow think tanks, and outside experts a working model that will be of real value to all.

The First Year—Process and Premise

During the first year of this project principal coinvestigators Arnaud de Borchgrave and Tom Sanderson met with current and former national intelligence directors, security service chiefs, nongovernmental experts, and journalists in seven European countries and in Morocco to discuss multilateral information and intelligence sharing on counterterrorism. They interviewed over 100 ranking officials who are or have been involved in counterterrorism. Without exception, they all said that multilateral intelligence sharing—in addition to the traditional bilateral sharing between two national intelligence services—was essential for dealing with a new class of threat. However, all recognized that this would take time to bring about, beginning with sharing among the national agencies of one country, as the United States has attempted to do with the National Counterterrorism Center (NCTC) and the United Kingdom with the Joint Terrorism Analysis Centre (JTAC), both of which have now been emulated in several European countries. These efforts are focused on the formidable problem of sharing classified information and continue to run into the obstacles that have been associated with this issue for years.26

As a surrogate, perhaps, for the conundrum of the classified, OSI presents an opportunity both to take smaller steps in information sharing regimes and practices and to provide new information of high value to counterterrorism efforts. The post-9/11 intelligence reform commissions, as previously noted, highlighted the immediate and dire need to expand and coordinate the collection, integration, and use of OSI. The intelligence community began to take those steps with the establishment of the Director of National Intelligence Open Source Center in the fall of 2005.

The creation of a model for trusted information networks by CSIS has the potential to provide real assistance to the intelligence community and its customers. Already, those who understand the root causes of the United States’ terrorist dilemma suggest that a “global war on terror” is, in Olivier Roy’s words, a metaphor, not a policy, because it risks infusing local disputes with the Islamist extremists’ millennialist goals. This has already happened. The old rallying cry of Palestine is now joined by the new one of Iraq. And both are overlaid on one enduring mantra—Islam cannot prosper so long as it is confronted globally with the suffocating hegemony of Western economic and cultural dominance.

Cynically manipulated or not, the Palestine issue has clearly helped create a constituency in the Muslim world dedicated to attacking Israel’s primary supporter, the United States. OSI contributors wonder what the global jihad’s current strength would have been had its chief enemy not been tainted by Guantanamo, Abu Ghraib, and other self-inflicted wounds.

---

26 The United States and France established in Paris, with the cooperation of Canada, Germany, the United Kingdom, and Australia, a counterterrorism analysis and coordination center called “Alliance Base.” See Dana Priest, “Help from France Key in Covert Operations,” Washington Post, July 3, 2005.
Gilles Kepel says that underlying all Islamist extremist rationalizations is the historical Muslim fear of *fitna*, a word meaning internal schism, sedition, and chaos. The traditional role of religious scholars was to guard against this menace. But, having arrogated to themselves the right to take the offensive against the *fitna*-creating West, these extremists have in fact inflicted *fitna* on their own societies. This is only one example of a geopolitical opportunity that OSI can illuminate for policymakers as they attempt to extricate the United States from the Iraqi quagmire.

In stark contrast to the Cold War era, a much greater understanding of the non-secret aspects of today’s threat environment is a prerequisite for understanding the remaining “secret elements,” which are crucial to security. Suitably refined and enhanced through a trusted information network, OSI can help provide those insights.

Intelligence analysts, of course, access a wide variety of newspapers, magazines, and radio and television newscasts from all over the world, courtesy of the Foreign Broadcast Information Service (FBIS) and LexisNexis, among others. But analysts have a cultural bias for classified information, which is seen as more important and more reliable. What is missing from the variety of publicly available information is the dynamic exchange and interaction of multiple experts from multiple disciplines working to understand an issue because it enhances their own work. The TIN aspect of the current CSIS effort brings this “expert” dimension to the table along with new sources of OSI that go beyond the traditional.

OSI enables the analyst to observe and penetrate the enemy’s thinking and understand how he sees his operational choices. European, North African, and Middle Eastern professors and social scientists have befriended would-be terrorists, monitored their favorite Web sites, and built impressive databases in French, English, and Arabic. They have captured many of the most telling strategic and tactical insights of Islamists through these unclassified efforts.

The original homegrown terrorists of the post–Cold War era were members of the Japanese politico-religious sect Aum Shinrikyo. They signed up some 10,000 members in Japan and another 15,000 in Russia, many with advanced university degrees; conducted biological experiments on animals on a large ranch the sect owned in northwest Australia; and sent their chief engineer 13 times to Russia in a futile quest to purchase a nuclear weapon. Aum’s chief guru, Shoko Asahara, mesmerized his followers with a blend of Buddhist, Shinto, and Christian phrases. His aim was to collapse capitalism in Japan, which he believed would trigger a fatal shock to global capitalism and globalization. Yet no intelligence service, Japanese or foreign, knew anything about this lethal sect until its followers attacked the Tokyo subway system in 1995 with sarin gas, killing 12 commuters and injuring thousands.

September 11, 2001, was also a dramatic wake-up call for a threat that had become global in scope, and the intelligence community was ill-prepared to face a widespread, long-term, and potentially catastrophic threat from militant Islam. As
the earlier U.S. struggle with communism suggests, the new threat may persist for several generations.

As the accelerating spread of nuclear technology portends, the stakes of this threat may involve the destruction of one or more of the United States’ great cities and perhaps even the very functioning of American society itself. The global network of Islamist terrorists has been energized and widened by the insurgency in Iraq. The result is a global Islamist campaign directed at the United States, its allies, and the West more generally.

To understand the correlation and interaction of these forces, an open source, trusted information network for counterterrorism would provide what this project’s investigators and a variety of individuals and intelligence experts concluded is the “missing dimension of intelligence.”

What Did We Find?

Transnational terrorism is an unbounded, poorly understood, and increasingly dangerous threat, and U.S. military, intelligence, and law enforcement agencies remain ill-prepared to counter it. While there are many causes for this, primary among them is the tendency of Western policymakers so far to view the problem as emanating from a finite number of “bad characters” who, when confronted with force, will either die on the battlefield or retreat to more acceptable behavior. And the moderates in Islam, under this logic, will emerge from hiding and set things back on their proper course. Unfortunately, reality does not support this view, and each day the reach of these extremists grows, even as the military, intelligence, and law enforcement agencies score their great successes. In December 2005, the United States proudly announced the killing (by a missile from an unmanned drone) of Rabia, the Al Qaeda chief of operations. He was the third Al Qaeda chief of operations killed since September 11, 2001.

The fact remains that in the four years since September 11, these agencies have been, in essence, the primary forces arrayed by the United States against terrorism and have been operating with only a partial understanding of the problem they face. They leave, however, significant voids in what must become a more comprehensive, multidimensional counterterrorism campaign. In order to fill these gaps, the government must reach beyond federal resources and expertise and draw on the deep knowledge of those with an understanding of this complex threat, as well as on an abundance of important open source information. That notion is the heart of the CSIS study.

The depth and scale of the terror threat confounds most people; it is an unfamiliar and forbidding subject that is rooted deeply in social, scientific, anthropological, religious, and cultural issues that are often unexplored by intelligence services. The languages spoken by many terrorists are not commonly found within the national security community. Terrorist tactics, organization, and motivations are not intuitive to Americans and test the United States’ capabilities as few adversaries have in the past. These areas are, however, the province of hundreds of experts from around the globe. Traditional government
counterterrorism and intelligence collection methods cannot be properly applied without the understanding and calibration that OSI and networked outside expertise can provide.

Ironically, this is well understood by many within the intelligence and policy communities, yet these tremendously valuable resources are underused, undervalued, or sometimes ignored despite the serious, persistent threat of terrorism. When properly integrated with intelligence held by government analysts, knowledge generated from a multilateral, multidisciplinary approach to information collection and sharing can play a decisive role in the response to many national security problems. Today’s threats are far too complex, opaque, and alien to Americans, Europeans, or Asians faced with our traditional dependence on classified intelligence. This was an effective formula during the Cold War and explains, in part, why governments still tend toward inward-looking approaches in their counterterror efforts. Unfortunately, it has met with minimal success today.

The continued failure to fully utilize OSI stems from:

1. continued implicit belief that “secret” information from clandestine sources must, somehow, be more valuable and accurate than that from a more open environment;
2. the difficulty (technical and cultural) of integrating open source materials into an environment that is almost exclusively composed of classified information sources, and;
3. the apparent failure to recognize that the new, unbounded threats from international terrorism, which now characterize the national security environment, represent a different threat environment and one that requires a major focus on open source collection to complement the rare but highly valuable insight derived from covert collection.

The transformation of the primary threat from the Soviet Union to transnational terrorism, and the lack of corresponding adaptation in our intelligence capabilities and information sources, highlights the dilemma we now confront. The old and the new threats are usefully contrasted as follows.

<table>
<thead>
<tr>
<th>The Problem We Faced</th>
<th>The Problem We Now Face</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bounded threat</td>
<td>Unbounded threat</td>
</tr>
<tr>
<td>Hierarchical operation</td>
<td>Decentralized, nodal trust-based relationships difficult to penetrate</td>
</tr>
<tr>
<td>Symmetrical threat with multiple observables</td>
<td>Asymmetrical threat with few and difficult observables</td>
</tr>
<tr>
<td>Intelligence approaches, emphasizing clandestine collection, designed to capitalize on these attributes and penetrate the core</td>
<td>Intelligence approaches designed to capitalize on these attributes and penetrate the core have yet to be developed</td>
</tr>
</tbody>
</table>
The intelligence community now must focus on areas that were of secondary interest during the Cold War. As such, the intelligence community lacks deep and historical expertise in the relevant disciplines and geographic regions. Traditional intelligence collection alone—by secret means, technical or human—will not meet the challenge of extremist terror groups that are profoundly difficult to comprehend, collect against, penetrate, deter, and defeat. Counterintuitive as it seems, open source information broadly construed will be at least as important in the world’s counterterror efforts as secret intelligence was during the Cold War.

Although many in the intelligence community are well aware of—and often use—open source information and the universe of experts outside the classified world, there is no comprehensive approach to exploiting this information and talent. Outside experts are most often engaged and consulted on a one-off basis, rather than as core, central participants in the intelligence process. According to a senior CIA official, the analysis model in the intelligence community has been “sit, think, and write.” Instead, said this official, it should be “reach out, debate, integrate, think, and write.”

Two Important Conferences

In addition to the extensive interviews with intelligence professionals and others in Europe and the United States and frequent meetings with study team members and others, two major conferences were held in Oslo and Brussels.

Oslo Framing Conference

On October 20, 2004, CSIS gathered 40 academic, diplomatic, intelligence, judicial, military, and private-sector leaders in Oslo, Norway, to discuss the findings from the first three months of interviews and research. Conference participants, as with many of those interviewed in the first three months, viewed the establishment of true multilateral intelligence sharing as a “bridge too far” and instead offered an alternative approach. That approach would entail a directed and comprehensive outreach to global expertise in numerous fields with bearing on terrorism and the fundamentalist elements that enable it. This information would be shared within a network (which the intelligence services would have access to under certain arrangements) and rely heavily on open sources.

A greatly expanded focus on OSI and trusted networks of experts was viewed as fundamentally necessary before any wholesale intelligence sharing could occur. Moreover, the use of OSI and trusted networks of experts was seen as more important in some respects than the sharing of intelligence due to its much richer perspective and ability to provide context to the terror threat. Most importantly, OSI is essential to guide more traditional sorts of intelligence collection in a universe that is far too complex to approach unaided.

The experience and feedback in Oslo launched CSIS in a new and even more relevant direction. With this new concept in mind, project leaders Arnaud de Borchgrave and Tom Sanderson, as well as the project’s core advisory group, developed a template for an OSI-based trusted information network that could directly benefit government counterterrorism efforts. In essence, this step takes
OSI beyond the traditional, static universe of databases (“LexisNexis on steroids,” as one participant put it) and instead incorporates the world of those databases into a dynamic network of substantive experts who are already working on disparate aspects of the same problem. This adds value to the knowledge and information available to the work of the individual experts themselves and the overall understanding of the underlying problem set.

**Brussels Workshop**

In May 2005 in Brussels, Belgium, CSIS gathered several participants from the Oslo conference in addition to key individuals responsible for the EU response to terror threats. Nongovernmental experts were also a vital component of the Brussels event. All participants possessed varied perspectives on these matters and contributed much to the daylong exercise and discussion.

Demonstrating the impact of a wide and diverse range of participants, the workshop benefited greatly from the tremendous insight and unique experience of a human rights consultant and journalist who, according to a colleague, “has spent more time in war zones, refugee camps, and among displaced persons than anyone should safely do.” This individual traveled from east Africa to join the CSIS workshop in Brussels. That individual’s presence and expertise were complemented by that of another participant who is an expert on immigration policy and the flow of people to and from Europe. Their interaction and contribution provided a clear affirmation of the importance of diverse expertise in the makeup of the trusted information network.

The ultimate goal of the CSIS workshop in Brussels was to design and plan the launch of a trusted, multinational terrorism information network. Brussels participants reiterated that the proposed network would have to bring clarity to issues being worked on by intelligence analysts, while helping them avoid the burden of sorting mountains of raw, open source information. To be successful, it would also have to bring value to the nongovernmental experts who comprise the TIN. The active and enthusiastic interplay among participants with widely different skills in Brussels and the substantive insights they provided gives us confidence that such a mix of expertise would prove effective.

Through the dynamic interaction of individuals in the network, insight and context will be lent to issues identified as important, shared problems. The Brussels exercise also validated the notion that, if properly designed, the experts in the network would sort the information in imaginative and nontraditional ways. This, in turn, produced a wealth of interesting and novel suggestions for areas of investigation; unique, nongovernmental experts; relevant though not obvious areas of expertise; and potential organizations that could offer substantive input or cohost future open source TINs. These immediate and fascinating results were instructive; participants and organizers alike saw great promise in this approach. (The appendix to this report captures informal ideas and suggestions emerging from the exchanges among experts in Brussels on the sorts of areas to which such a TIN might devote attention as the project progresses. The listing is of interest as it demonstrates those areas of importance to understanding and combating
terrorism that are not likely to be available through traditional intelligence means but, when melded with those classified elements, may provide greater understanding of the overall threat.)

Team members were in frequent contact with both U.S. and key foreign intelligence community members. This interaction and guidance contributed substantially to the success of the study and is all the more important in view of the underlying objective—develop a working open source/trusted information network model that can be used by governments to enhance their performance against the threat of terrorism.

The Second Year—What Do We Propose?

The most striking element of the first year’s investigation was the widely held view that a new, alternative, promising, and equally important approach to counterterrorism should be taken. Significantly, the senior European and American intelligence and security leaders contacted by the principal investigators in the early stages of the project found themselves in unanimous agreement regarding the importance of this approach. Further, they believed that combining OSI and a multinational, multidisciplinary, trusted network of government and nongovernment specialists would provide an important service to policymakers and intelligence officials now. This type of global, wide-ranging, and dynamic sharing of publicly available information was suggested as an indispensable element for global counterterrorism efforts.

The consensus was that multilateral sharing—in addition to the traditional and generally effective bilateral arrangements between national intelligence and security services—was needed immediately. By focusing initially on the importance and utility of “information” (as distinct from “classified intelligence”) those interviewed suggested that this would speed the eventual dawn of true multilateral intelligence sharing. In the meantime, the focus on information sharing among multiple nations and individuals would elicit the type of knowledge that is highly valuable (and largely absent) in current counterterrorism efforts.

OSI, many commented, provides critical peripheral vision to a terrorist threat that is multifaceted and does not lend itself to overreliance on any one collection technique. OSI is also highly valuable because it can be distributed more easily between federal, state, and local officials, many of whom rarely have security clearances. This is of increasing importance for the United States, as more power and demands are being focused on, and driven by, state and local homeland security officials.

Follow-on Steps

CSIS, in 2006, has embarked on a project that seeks to:

1. complete the identification of relevant open sources of information, especially nontraditional source in such areas as sociology or
anthropology that are essential to understanding the reality of potential terrorist group growth and practices in our societies today;

2. examine the utility of such entities as Web logs (“blogs”) to serve not only as a static source of information, but also as a virtual depiction of the dynamics that change and transform these organizations;

3. determine, through the actual operation of a trusted information network, how practitioners in one area (e.g., sociologists researching suicide bombings) can reinforce—and themselves be reinforced by—practitioners in an ordinarily unrelated area (e.g., nongovernmental immigration experts covering crime issues among émigré communities in a given country).

This second-phase operation will not only expand and refine the work completed in the first phase, but the operational TIN will directly enable the dynamic interaction of experts from multiple disciplines seeking to understand challenges that are central to their work and those of governments.

The TIN consists of roughly one dozen specialists in diverse fields of expertise broadly related to the underlying elements of radical transnational terrorism. For a period of several months participants will share open source information and insights on the roles, activities, and impact of Islamist extremists on European security. Importantly, this effort will consider, but not be limited to, an examination of the influence of those Muslim fundamentalists who return to Europe after fighting in Iraq, Afghanistan, and other areas. CSIS will moderate this interaction, including establishing and ensuring guidelines for information exchange and adding substantive input to the dialogue where appropriate. The seven-member core advisory group will also actively participate in the discussion, adding their tremendous expertise and networks to this effort.

Frequent, periodic reviews are scheduled, as is a mid-term review and a concluding conference, to examine conclusions and their value to TIN participants and governments and to gain insights on the terrorist threat and the open source, trusted information network process. A final report will outline how harnessing and sharing experts’ open source knowledge can offer a tremendous bounty of information for counterterrorism efforts.

Conclusion

The next major terror attack will, with near certainty, involve terrorists from multiple cities, with networks in several countries, spanning two or more continents. Terrorists will finance their operations with cross-border trafficking, street crime, and contributions from sympathetic individuals worldwide. If additional terrorist funds are needed, they will be transferred by the opaque and ubiquitous Hawala money transfer system that is immune to the West’s sophisticated terrorism finance countermeasures. Weapons will be made and stored in communities where police fear to tread and where local activities and movements can only be understood and noticed by those who live there. Terrorists will speak languages (often with code) rarely known by those trying to
stop them and will ply an immensely complex Internet that serves as a force multiplier. Their use of modern technology along with traditional culture and social networks will afford them great advantage over governments bound by regulations, borders, and bureaucratic rivalries that make countering terrorism extremely challenging.

These confounding factors and capabilities can only be understood and confronted by government analysts and counterterrorism forces who undertake a comprehensive program to engage dynamic networks of experts and to integrate knowledge drawn from open source information. In conjunction with classified intelligence, these two publicly available sources of information and expertise will provide a more detailed picture of the terrorist threat. Additionally, nations tracking potential threats will have to begin sharing this combination of classified intelligence and open source information with one another. Not doing so for fear of leaks or unreliable information could have catastrophic results.

CSIS embarked on this timely project during the course of high-level government reviews of intelligence failures. Those reviews called for a much greater exploitation of open source information that could be of particular use in counterterrorism. Our second-phase study will heed this call while providing a working model for outreach and coordination with nongovernmental specialists. Ultimately, we hope to move democratic governments closer to the multilateral, all-source information and intelligence sharing necessary for a decisive impact on transnational terrorism.
Appendix

Potential Areas of Investigation for the CSIS Trusted Information Network

- Terrorist group infrastructure
- Mobilizing Islamic and Arab women—what role can they play in counterterrorism?
- Public health issues
- Second generation Muslim fundamentalists
- Emerging impacts on the threat of terrorism (future counterterrorism measures)
- How terrorist groups react to government control measures
- How internal dynamics change under counterterrorism pressures—what is the change and what exerts the greatest force?
- What is going on in the mosques?
- What does the terror problem suggest about Muslim émigré populations in Europe?
- Suggestions that enclaves are volatile—what does this mean for immigration?
- How do you legally move materials intended for illegal purposes?
- How do the war in Iraq and the situations at Abu Ghraib and Guantanamo affect Islamic extremist recruitment?
- Al Jazeera and its impact on youth
- The leakage of nuclear materials and warheads
- What do these movements look like, what are their critical nodes, which people can we act on—viewing terrorism from an enterprise perspective
- Synthesizing anthropology and religions of hinterland groups
- Discerning differences between criminally inspired activity and other motivations for crime
- Relevant financial transactions of immigrant communities
- Low-cost, flattened terrorist structures and the link between terror and crime
- Funding localized terrorist activity--the need to “know the enterprise”
- Hawalas—how do they really work?
- Questions about Islam and its challenge by radicals
- What are the ideological underpinnings of moderate Islam?
- Have outside experts draw out knowledge on suicide bombers
- Recruitment of young Americans or Europeans for terror strikes
- Mitigating short- and long-term effects on financial markets of the next major set of coordinated attacks
- Arabic and terrorist Web sites—collect widely available information on terror groups and use it to develop a better picture of them
- High-value targets from the terrorists’ point of view
- Expand work on the sociopolitical background of terrorists
- The gem trade and terrorism (diamonds)
- Steganography
- Massive multiplayer on-line games (used for terrorist training)
- Why have we not seen attacks with bio-weapons?
- How do terror groups target multinational corporations?
- How to build resiliency and confidence in our communities?
- What makes the bad guys tick, but also, what makes us tick?
- Risk communications
About the Authors

**Arnaud de Borchgrave** is director of the CSIS Transnational Threats Project. During a 30-year career at *Newsweek* magazine, he covered most of the world’s major news events. At 21, he was appointed Brussels bureau chief of United Press International (UPI), and three years later he was *Newsweek*’s bureau chief in Paris. At 27, he became senior editor of the magazine, a position he held for 25 years. He was appointed editor in chief of the *Washington Times* and *Insight* magazine in 1985. He left his post with the *Washington Times* in 1991 and currently serves as its editor-at-large. He served as president and CEO of United Press International from 1999 to January 2001. He is currently serving as editor-at-large at UPI. While at CSIS, he coauthored *Cyber Threats and Information Security* (2001), *Russian Organized Crime and Corruption* (2000), *Cybercrime, Cyberterrorism, Cyberwarfare* (1998), and *Global Organized Crime* (1994).

**Thomas Sanderson** is deputy director and fellow of the Transnational Threats Project, where his work focuses on intelligence and information sharing; terrorist groups, operations, and crime; and U.S. national security policy. In 2005, he completed a Bosch public policy fellowship at the American Academy in Berlin. Prior to CSIS, Sanderson served as a defense analyst with Science Applications International Corporation, where he studied terrorist groups for the U.S. Defense Intelligence Agency, Office of Counterterrorism Analysis. He also held the 2001 Henry L. Stimson Center fellowship at Fudan University in Shanghai, China, and spent four years helping to develop nongovernmental organizations in Central Asia and Russia. Sanderson is a terrorism course instructor, lecturer, and consultant for the U.S. government, private sector, media, and academic communities. He holds a B.A. from Wheaton College in Massachusetts and an M.A.L.D. from the Fletcher School of Law and Diplomacy at Tufts University.

**John MacGaffin** is a senior adviser to the Transnational Threats Project. He served for almost 40 years with the CIA, where his postings included four assignments overseas as chief of station, primarily in the Middle East, and at CIA headquarters, as head of strategic planning and evaluation, chief of the Central Eurasian operational division, and associate deputy director for operations, the second-ranking position in the nation’s clandestine intelligence service. After leaving the CIA, he became senior adviser to the director and deputy director of the FBI, with responsibility for long-range enhancement of CIA/FBI relationships. Beginning in 1998, he chaired a commission on behalf of the secretary of defense, the director of central intelligence, and the director of the FBI to restructure the national counterintelligence system. MacGaffin has served on the Defense Science Board Taskforce on Homeland Security and its Taskforce on Intelligence in Support of the War on Terrorism. He is also a member of the Steering Committee of the CSIS Project on Transnational Threats, serves on the Board of Advisers for the CSIS Open Source Intelligence Network Project, and is intelligence adviser to the National Infrastructure Advisory Council.
OPEN SOURCE INFORMATION
The Missing Dimension of Intelligence

A Report of the CSIS Transnational Threats Project

Authors
Arnaud de Borchgrave
Thomas Sanderson
John MacGaffin

March 2006

ISBN-10: 0-89206-483-8