Combating Terrorism and Its Implications for Intelligence

FRED R. SCHREIER

> *"Terrorism is a global threat with global effects … Its consequences affect every aspect of the United Nations agenda—from development to peace to human rights and the rule of law…. By its very nature, terrorism is an assault on the fundamental principles of law, order, human rights, and the peaceful settlement of disputes upon which the United Nations is established…. The United Nations has an indispensable role to play in providing the legal and organizational framework within which the international campaign against terrorism can unfold."*
>
> —Kofi Annan, UN Secretary-General, 4 October 2002

Terrorism has been of concern to the international community since 1937, when the League of Nations elaborated the Convention for the Prevention and Punishment of Terrorism. Subsequently, the UN and other intergovernmental organizations have dealt with terrorism from a legal and political perspective. Since 1963, the international community has elaborated twelve universal legal instruments related to the preven-

tion and suppression of international terrorism, many initiated by the United States.[167] Regional organizations such as NATO, the EU, OSCE, SAARC, and ASEAN have made counterterrorism a principal concern. And new organizations such as the Shanghai Cooperation Organization have provided guidance and cooperation.

Yet grievous incidents recorded in recent years in such disparate places as Paris, Jerusalem, Oklahoma City, Algiers, Dhahran, Lima, Karachi, Nairobi, Dar-es-Salaam, New York City, Washington D.C., Bali, Djerba, Casablanca, Riyadh, Istanbul, and Madrid – accompanied elsewhere by a myriad of less serious ones – dramatically confirm that in the twenty-first century, no country, society, or community is immune to terrorism.

While it is difficult to judge how successful the overall counterterrorism effort has been, inevitably there has been public discussion of the question of whether 9/11 and subsequent attacks were "intelligence failures."[168] The enquiries in the United States into the performance of the

---

[167] On 12 September 2001, the UN General Assembly, by consensus of the 189 member states, had called for international cooperation to prevent and eradicate acts of terrorism and to hold accountable the perpetrators of terrorism and those who harbor or support them. The same day, the Security Council unanimously determined, for the first time ever, any act of international terrorism to be a threat to international peace and security. This determination laid the foundation for Security Council action to bring together the international community under a common set of obligations in the fight to end international terrorism. On 28 September 2001, the Security Council unanimously adopted resolution 1373 under chapter VII of the UN Charter. This established a body of legally binding obligations on all member states. Its provisions require, among other things, that all member states prevent the financing of terrorism and deny safe haven to terrorists. States were asked to review and strengthen their border security operations, banking practices, customs and immigration procedures, law enforcement and intelligence cooperation, and arms transfer controls. All states are required to increase cooperation and share information with respect to these efforts. The Resolution also called upon each state to report on the steps it had taken, and established a committee of the Security Council to monitor implementation. In October 2002, The Global Program against Terrorism was launched as a framework for UNODC's operational activities working through technical assistance projects on Strengthening the Legal Regime against Terrorism. The UN Office on Drugs and Crime is committed to deliver tailor-made assistance through: (1) reviewing domestic legislation and providing advice on drafting enabling laws; (2) facilitating and providing training to national administrations with regard to new legislation; (3) providing in-depth assistance on the implementation of the new legislation against terrorism through the mentorship program; and (4) maintaining a roster of experts to supplement specific expertise where required. See http://www.undoc.org/undoc/en/terrorism.html.

[168] A good analysis of the phenomenon of intelligence failures can be found in: Betts, Richard K. Jr., "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics* (October 1978).

intelligence community in the months preceding 9/11 uncovered both specific shortcomings and systemic weaknesses in intelligence performance[169] and have led to three major findings:

- The new indiscriminate terrorism, as represented by Al Qaeda and its associates, poses a major threat not only to the United States and its presence abroad and to the national security of individual nations, but to regional and international peace and security.
- The traditional counterterrorism approach of viewing terrorism as a phenomenon, which can be prevented and controlled by better identification and redressing of grievances, better governance, enhanced economic development, and measures to win the hearts and minds of the people, would be inadequate against the new indiscriminate terrorism. Many of those who have taken to the new terrorism come from well-to-do families, and economic deprivation and social injustice were not among the root causes of their terrorism. Since some of their pan-Islamic objectives—such as the creation of regional Islamic caliphates ruled according to the Sharia—cannot be conceded by the international community, there is a need for a more robust counterterrorism approach to neutralize these organizations.
- The national intelligence agencies, by themselves, however strong and capable, may not be able to deal with this new threat of international terrorism. Hence, the need for an interagency framework for planning, executing, and coordinating counterterrorist efforts, and improved regional and international intelligence sharing and cooperation between the intelligence and security agencies to counter these terrorist networks. Thus, the new terrorism calls for revamped intelligence apparatuses at the national level and reinforced coordination mechanisms at the regional and international levels.

But what has been the public perception of the counterterrorism performance of national intelligence and security services before 9/11 and thereafter? The common complaint against intelligence and security agencies in all countries confronted with the scourge of terrorism has been that the agencies, while effective and efficient in detection and investigation after a terrorist act has been committed, have been wanting in their abilities to prevent a terrorist act.

Yet it would be unfair to the intelligence services to say that they are not able to prevent acts of terrorism through timely intelligence. For every successful act of terrorism, there are others thwarted by

[169] See Best, Richard A., Congressional Research Service Report RL31650, *The Intelligence Community and 9/11: Congressional Hearings and the Status of the Investigation*, updated 16 January 2003.

the agencies, either through timely intelligence or effective physical security.[170] Details of many of these are regularly kept outside public knowledge in order not to compromise the sources or reveal the methods and professional techniques used by the agencies.

Despite this, it is normal that public opinion would judge the intelligence and security agencies not by their unannounced successes, but by their well-known failures. And failures there have been in plenty: not only in developing countries, but also in the United States and in Europe, despite their far greater financial resources and their more sophisticated technological capabilities. The world is also witnessing continuing terrorist strikes by Chechen groups in Russia and the unending wave of terrorist incidents in Iraq since May 2003, which speaks of continuing failures of the Russian and the U.S. intelligence communities. Though different terrorist organizations are responsible for these incidents, all of them have a similar *modus operandi*, involving the use of explosives activated through either timers, remote control devices, or suicide bombers.

What are the problems in combating terrorism, what are the possible remedies, and what are the implications for intelligence?

Key issues:
- What is the essence of combating terrorism?
- What makes combating twenty-first century terrorism so difficult?
- What are the challenges and problems for intelligence?
- Is there a need for a new approach to intelligence?

What Is the Essence of Combating Terrorism?

Terrorism is the societal evil of our time, which must be combated as slavery and piracy were in the nineteenth century and fascism and apartheid in the twentieth century. Efforts to disrupt and destroy terrorist organizations occur in many ways: diplomacy in bilateral and multilateral fora; law enforcement efforts to investigate, arrest, and prosecute terrorists; financial and other measures to eliminate terrorist support;

[170] See for example "Oplan Bojinka," a complex plan to bomb eleven U.S. airliners over the Pacific as they travelled from Asia back to the United States. More than 4,000 people likely would have died had the plot not been discovered in 1995. A multifaceted attack on the Los Angeles airport and other U.S. related targets to coincide with millennium celebrations in January 2000 was foiled as a result of a chance apprehension of an individual with a car loaded with explosives by an alert customs service official. Attacks on U.S. embassies and facilities in Paris, Singapore, and other parts of the world have been thwarted because of intelligence leads.

military actions to destroy terrorists and regimes that harbor them; and covert operations by intelligence services.

The essence of combating terrorism can be found in the many strategies existing.[171] Most contain comparable content to the U.S. National Strategy for Combating Terrorism,[172] which claims leadership in the worldwide effort and is the most offensively oriented. For the United States, the best defense is an aggressive offense, in which traditional counterterrorism, antiterrorism, intelligence collection, and covert action are seamlessly integrated. All strategies seek to create a global environment hostile to all terrorist groups, whether they operate globally, regionally, or within the boundaries of a single state. They provide guidance to orchestrate all instruments of national power while coordinating the collective efforts of the international community. The end state of the strategies is invariably a world free of terrorism as an instrument of societal change and a global environment in which terrorism can not flourish again.

Since the fight against terrorism requires a multidimensional, multinational approach aimed at the entire spectrum of terrorism, the strategies call upon states, international and regional organizations, private and public entities, and individuals to collaborate in combating terrorism at all levels simultaneously. The UN should lead the effort while facilitating regional responses and assisting individual partner states. The goal is to reduce terrorism to a level at which it can be combated as mere crime.

All strategies place primary responsibility on sovereign states that have jurisdiction over terrorist activities within their borders. Many states are well equipped to combat terrorism. Others are weak and require assistance. A few are ambivalent or reluctant and require motivation. Some states still support or sponsor terrorists and must be compelled to stop. Thus the UN, NATO, and the EU, as well as the United States encourage all societies to pool diplomatic, informational, military, and economic capabilities to defeat terrorist organizations wherever they exist, deter future acts of terrorism, and ultimately diminish the underlying causes of terrorism through a concerted effort at the global, regional, and sovereign-state levels. At the same time, individual states are called upon to provide defense for their citizens at home and abroad.

---

[171] Issued by the UN, NATO, the European Council in May 2004, and other international and regional organizations as well as by individual states.

[172] *National Strategy for Combating Terrorism*, February 2003.

Defeating Terrorist Organizations

The first element of combating terrorism as an instrument of change aims at defeating existing terrorist organizations at the global, regional, and state levels. Terrorism will only be defeated by solidarity and collective action.[173] Through direct and indirect use of diplomatic, informational, military, and economic instruments of power, the international community should seek to defeat terrorist organizations by attacking their "centers of gravity," while directly compelling or indirectly influencing states that sponsor terrorists. The centers of gravity of terrorist groups include leadership, supporting ideology, finances, command and control networks, and sanctuaries. To defeat existing terrorist groups, the UN and the United States, its allies, and coalition partners need to:

- Identify and isolate terrorist organizations at each level
- Disrupt support infrastructure and sanctuaries
- Discredit ideology or reasons for committing acts of terrorism
- Destroy networks and leadership

While it is unrealistic to hope to eliminate every single terrorist who desires to threaten innocent individuals, it is possible to eliminate the synergy created by the cooperation of disparate terrorist organizations. This effort will reduce the operational scope and capabilities of global and regional terrorists to the point that they become threats only at the individual state level. At that level, the threat can be combated as criminal behavior, which will allow for a narrower focus of attack and enable the full engagement of law enforcement mechanisms.

Deterring Future Acts of Terrorism

The second element of the strategy focuses on deterring future acts of terrorism. To establish a credible deterrent, the international community should develop and maintain a set of capabilities and mechanisms that clearly communicate to potential terrorists and their supporters that their costs will far outweigh any perceived benefits of engaging in terrorism. The deterrence message should be sent not only to terrorist organizations but also to states that sponsor them, nonstate actors that provide a front for their activities, and individuals who may contemplate joining or supporting them. The goal of deterring terrorism supports the strategic aim of abolishing terrorism by convincing individu-

[173] European Council Declaration on Combating Terrorism, May 2004.

als, organizations, and states to seek alternative methods of political change because terrorism is no longer a viable option. Providing a deterrent message to each of the four audiences associated with terrorism requires:

Deterring terrorist organizations. Terrorist organizations believe that they can conduct operations with impunity. Capabilities, particularly improved intelligence, should be acquired to detect, thwart, and destroy such groups and bring their members to justice. Actions should be taken to create the certainty that terrorists will be captured and imprisoned rather than becoming martyrs for their cause. Political, social, and religious leaders must understand that their organizations will be destroyed if they choose terrorism to advance their aims.

Deterring state actors. States must be deterred from providing support or sanctuary to terrorist organizations. This can be done by broadening international norms against terrorism and demonstrating the resolve to replace the leadership of any state that continues to sponsor terrorism. States must clearly understand that the costs will far outweigh any perceived benefits of engaging in acts of terrorism.

Deterring nonstate actors. Nonstate actors must be deterred from providing aid and assistance to terrorist organizations. This can be achieved by establishing an international environment of greater financial transparency, naming and shaming organizations involved in terrorist support, and lowering the barriers to asset seizures and freezing of funds.

Deterring individuals. Efforts to deter individuals from joining or supporting terrorist organizations include educating potential recruits on the sinister nature of specific organizations and of terrorism in general, dispelling the notion that terrorism results in positive gain, and demonstrating that terrorists will be brought to justice.

Although some believe that terrorists are undeterrable, we can find arguments that prove the contrary. State and nonstate actors *can* be deterred from providing assistance. The tougher challenge applies to the actual terrorist organizations and their followers. Deterrence of these will take time. The bottom line is that terrorists must believe that ultimately their efforts would be futile.

Diminishing the Underlying Causes

The group of efforts to diminish the underlying causes of terrorism compose the third element of the strategy of abolishing terrorism as an instrument of change. Through an aggressive long-term campaign, the international community should mitigate the underlying conditions that foster the formation of terrorist groups and their support elements. To

do this, the international community should directly or indirectly engage vulnerable regions and disparate ideologies and peoples.

The major contributors to the underlying causes of terrorism are:
- Economic and social inequality in societies marked by both abject poverty and conspicuous affluence
- Poor governance and economic stagnation or decline that alienates many segments of a state's population
- Illiteracy and lack of education that lead to widespread ignorance about the modern world and resentment toward Western values
- U.S. and Western foreign policies, particularly regarding the Middle East, that have caused widespread resentment toward America and the West

To mitigate these underlying causes, the international community should renew efforts to address the causes by the following actions:

- Increase foreign development assistance and use it to promote accountable and participatory governance along with an environment favorable to sustained economic growth
- Promote literacy and education in the Islamic world and underdeveloped nations
- Engage in information operations to denigrate the concept of terrorism and discredit its supporting ideologies
- Reenergize efforts for peace and stability in the Middle East

Defending the State on the Home Front

On the home front, states should remain vigilant and ready by establishing collaborative relationships between the ministries, the agencies, law enforcement, public health and emergency management entities, professional associations, and private partners. To that end, states should use every power available to defend their citizens against terrorist attack. States should be postured to provide an effective defense in three areas:

Prevent terrorist attacks. To the maximum extent possible, would-be terrorists and the weapons they intend to use must be denied entry into the country. Weapons of mass destruction must be detected and intercepted before they can be employed. Collaboration at all levels of government, along with the participation of private sector and individual citizens, is essential to disrupting terrorist aims.

Protect critical assets. To minimize the probability of a successful terrorist strike, states should harden critical infrastructure and other po-

tential terrorist targets. Cyber-based attacks are a real threat to the nation's critical computer-supported infrastructures, such as telecommunications, power distribution, financial services, national defense, and government operations.

Prepare responses. To reduce the effect of terrorism, states should be prepared to mitigate the consequences of an attack. This is particularly critical when responding to attacks from weapons of mass destruction. Collaboration among all ministries, agencies at the federal, regional, and local levels is essential. States should be safe and secure at home to preserve the way of life, maintain economic growth and stamina, and remain engaged in the international effort against terrorism.

However, while there are strategies that contain the essence for combating terrorism, the strategies by themselves, no matter how cohesive and comprehensive, will not ensure an integrated and effective set of programs to combat terrorism.

What Makes Combating Twenty-First Century Terrorism So Difficult?

The motives behind twenty-first century terrorism are new. Globalization has enabled worldwide terrorism and has facilitated the development of worldwide goals. Rather than using terrorism to create change within a single society or focus on a specific government, terrorism has gone international to support global causes, and the United States and the West have become primary targets. Though the events of 9/11 saw terrorism produce its most destructive event to date, trends from the preceding decade indicated an increase in violence. Terrorist attacks are becoming increasingly sophisticated and are designed to achieve mass casualties, and the trend towards greater lethality will continue.[174] The difference, however, is more than an increasing magnitude of indiscriminate mass casualty attacks, deliberately targeted against civilians, noncombatants, and societies ever more vulnerable and dependent on functioning critical infrastructure: The terrorist threat is confronting all of society in the twenty-first century.

The new terrorists are backed by powerful organizations located throughout the world and have achieved a de facto sovereign status by acquiring the means to conduct war – and have in fact declared war – posing a significant military and foreign policy challenge for which the West had no preplanned response. With global motives, global capabil-

[174] *Global Trends 2015: A Dialogue about the Future with Non-government Experts*. NIC 2000-02 (December 2000).

ities, and the probable use of weapons of mass destruction, this really is a new kind of war.

Since the new terrorists are trying not only to coerce or intimidate governments or societies but also to create an environment that unites a larger Muslim population against Western ideals and societies, the world is seeing a global insurgency aimed at ultimately altering the global balance of power, with the West being caught up in "somebody else's civil war."[175] In almost every Muslim country, there are calls by conservative religious elements for the revival of very old traditions. These elements view modern Western civilization as threatening the survival of traditional Islam as Western civilization bolsters the real enemy – secularism. The struggle is not new, but the identification of the United States and the Western world as an ally of the enemies of Islam has gathered momentum with U.S. and Western policy support for secular, corrupt regimes throughout the Middle East and with the Palestinian-Israeli conflict. Civil wars are agony for all participants, and they tend to last longer than other wars. The struggle between secularism and Muslim tradition will likely last at least a generation or more.

Moreover, the concept of global insurgency applies not to a single terrorist organization but collectively to many terrorist organizations throughout the world. These organizations have established a global, interconnected network of operations that often provides mutual aid and support in which it is difficult to isolate a particular group or faction without drawing linkages to other organizations that provide direct support, indirect assistance, or pursue similar goals. States with poor governance, ethnic, cultural, or religious tensions, weak economies, and porous borders will remain prime breeding grounds for the new terrorism. In such states, domestic groups will challenge the entrenched government and transnational networks seeking safe havens. At the same time, the trend away from state-supported political terrorism and toward more diverse, free-wheeling, international networks enabled by informational technology will continue. Some of the states that sponsor terrorist groups today may decrease or cease their support as a result of regime changes, rapprochement with neighbors, or the conclusion that terrorism has become counterproductive. But weak states also could drift toward cooperation with terrorists, creating de facto new state supporters. Moreover, there is also a coalescence of terrorism and other transnational crimes, which provide terrorists with various sources of income to finance their operations. These include, for example, illegal immigration, contraband smuggling, visa fraud, piracy, human traffick-

[175] Doran, Michael, "Somebody Else's Civil War," *Foreign Affairs* 81, no. 1 (January-February 2002).

ing, diamond smuggling, and tobacco diversion and associated tax fraud.

Terrorist groups operating on their own in loosely affiliated groups have increased. In particular, Islamic terrorist groups tend to be loosely organized, recruit their members from many different countries, and obtain support from an informal international network of like-minded extremists. The resulting transnational and decentralized structure helps terrorists avoid detection. The new brand of international terrorism more closely resembles a virus that mutates as its environment changes. Individual subgroups are capable of evolving their own strategy, and gaming their opponents. And if hit, the adversary will adapt, regroup, generate new leadership, shift geographic locus, adjust tactics, and evolve into a new collection of cells and networks capable of self-healing, dispersal, reassembly, and innovation.

The overall strategy of the new terrorist groups recognizes that they are in an inferior power position and must strike asymmetrically while winning sympathies from other terrorist organizations, governments aligned against the West, and the larger Islamic population. But time is on their side. In support of their insurgency, they have adopted a transnational strategy characterized by its global, protracted, diffuse, decentralized, complex, and ideological attributes. Buttressing the strategy are the sophisticated exploitation of modern media and technology, telecommunications, antiglobalization sentiments, indoctrination techniques, and a recruitment pool of disenfranchised Muslims. These terrorists aim for support from active participants, who plan and conduct highly compartmentalized terrorist operations, and passive sympathizers, whose silence does not betray or impede the insurgents. Appeals to the masses are effective in broadening passive support, as well as gaining "troops" whose orders to fight may take them to a variety of terrorist battlefields, such as Afghanistan, Iraq, Kosovo, Kashmir, Chechnya, the Philippines, Indonesia, or sub-Saharan countries. Furthermore, global terrorism has been highly successful in influencing the intelligentsia of the Muslim world, whose passive support is particularly critical in thwarting intelligence efforts and whose active support provides executive leadership, financial backing, and ideological legitimacy.

Personal, social, political, cultural, and religious causes for disunity within the groups are largely impenetrable to Western influence. As a result, the West will have to depend upon moderate Islamic leaders and opinion makers to discredit the interpretation of jihad adopted by terrorist organizations. To disrupt the new terrorists' ability to organize, plan, integrate, synchronize, and conduct future operations is a daunting task, given the scope and complexity of global terrorist organizations, which are present in more than sixty countries. The extensive network of schools and training camps will make it difficult to undermine the terrorist support that has been built up over the last several years.

The protracted struggle with the irregular force that represents one side of the "Islamic Reformation" presents a radical departure from all models of conventional warfare to which the West and its intelligence services have been accustomed. This struggle is daunting since defeating a broad-based, decentralized, and self-generating network like Al Qaeda is an unprecedented task. The following table[176] makes clear that the new enemy is of a completely different nature. This adversary is an evolving, adapting, and self-organizing[177] force and network with roots that spread everywhere, for which models of deterrence fail.

Self-Organized Terrorism Compared to Conventional Military Threats

Dimension	Conventional Military Threat	Self-Organized Terrorism
Organization	hierarchical, formal	flat, informal, networked
Leadership	concentrated, institutional authority	primarily symbolic, role in fundraising
Loyalty	a state and a policy	a tradition
Coalition partners	formal, perhaps shifting	informal, but likely enduring from conflict to conflict
Command and Control	centralized, with clear power relationships	decentralized, no one fully in charge
Role of intelligence	powerful, primarily offensive	weak, primarily defensive
Denial and deception	useful, but secondary importance	well developed, critical to mission
Doctrinal development	derived from formal study, historic experience, simulation, and gaming	evolutionary, trial and error
Other security obligations	numerous, including regional security, peacekeeping, formal alliances	none
Weapons arsenal	built through formal acquisition; takes years, even decades; resources abundant	adaptable, evolves quickly via natural selection; resources a constraint
Financing mechanism	formal budgets, funded by taxes	contributions from nongovernmental organizations, crime, narcotics

[176] Table taken from Harris, James W, "Building Leverage in the Long War," *Policy Analysis* 439 (16 May 2002).

[177] Self-organization refers to the propensity of the elements of a system to establish order without central oversight, as though doing so spontaneously. The idea is especially germane to biological and political systems, in which cells begin to work synergistically—in the early development of an organism or when a political movement is quickly "born" of commonly shared but only recently formed opinions. Financial markets also exhibit self-organization, when "bubbles" are created out of the dynamics of the expectations of individual participants. Networks also exhibit an emerging structure, as subgroups are added and connectivity multiplies disproportionately.

Terrorist organizations, ranging from those with global reach to those with merely local influence, support one another in an interconnected fashion. They are linked together in two distinct ways. The first is through *hard links* in which there is direct interaction and cooperation among terrorist groups. These links can eventually be detected, analyzed, and acted upon. The second is through *soft links*, which remain difficult to detect or influence.

Hard links: Terrorist organizations work together when it is in their interest to do so. These organizations may have different ideologies, goals, adversaries, or sponsors, but there may be compelling reasons to cooperate. Some of the hard links among these organizations are:

Financial support: occurs in many forms, from direct financial transfers to engaging in such mutually beneficial business deals as illegal drug trafficking or diamond sales, counterfeiting goods,[178] charitable organizations that funnel money to terrorist groups, and legitimate businesses that launder money from illicit sources.

Sharing intelligence: terrorist organizations sometimes share information regarding Western operations, critical vulnerabilities, intelligence collection methods, counterterrorism and counterintelligence capabilities, and political activities. They also share information to maintain situational awareness and improve the quality of their planning.

Coordinating activities: terrorist organizations have coordinated their efforts to maximize the psychological effect of terrorist operations or to demonstrate the ability to conduct sustained operations over time.

Sharing safe havens: a number of terrorist organizations operate training camps and maintain bases of operations near one another. Safe havens have been shared by like-minded terrorist organizations, taking advantage of governments willing to sponsor them.

Sharing materials and resources: terrorists exchange technology to construct bombs and the techniques to employ them. Key materials are also shared among some organizations. This becomes particularly worrisome as some terrorist organizations pursue the acquisition of weapons of mass destruction.

Sharing personnel: closely linked terrorist organizations share personnel for training or intelligence purposes or to develop a key capability within the organization such as encrypted or encoded communications, counterfeiting documents, or traveling incognito.

---

[178] Counterfeiting is estimated to yield some $600 billion a year for criminal organizations, including those that fund terrorists. Last year, law enforcement personnel in Lebanon seized $1.2 million worth of counterfeit brake pads and shock absorbers. According to a statement by Interpol chief Ronald Noble on 28 May 2004 in Brussels, the proceeds from their sales were destined for supporters of Hezbollah.

Soft links: This category characterizes the manner in which terrorist organizations operate without direct communications or coordination. Although difficult to delineate, some of the soft links are:

Sharing opportunities: as one organization strikes, other organizations may take advantage of an emerging opportunity.

Sharing responsibility: one organization may commit an act of terrorism while another organization claims responsibility. This may serve to confuse retaliation measures, cloak those who are truly responsible, and draw attention to the terrorist organization that elected to claim responsibility.

Public diplomacy: some terrorist organizations have access to or are able of influencing broad-reaching media mechanisms to communicate rationale or support for other terrorist organization activities.

Sharing ideological views: ideological leaders associated with a particular terrorist organization or a specific country sponsoring terrorism may communicate support to other terrorist organizations' activities or incite demonstrations supporting specific causes or opposing common foes.

In the aggregate, these hard and soft links work together to create a spectrum of terrorism that ranges from state-level terrorist organizations seeking to modify their government's behavior to global terrorists with worldwide hegemonic goals, ultimately striving to replace Western culture with their radical view of Islam. Due to these linkages, any viable counterterrorist strategy must embrace an integrated approach; hence the need to combat organized crime and terrorism collectively.

Organization tools such as ideology, leadership, recruitment pools, and publicity are necessary to sustain a terrorist group's existence as a cohesive entity. Operational tools such as command and control, weapons, training, intelligence, and money allow terrorists to conduct successful attacks. Understanding these factors may help identify the means of reducing a particular group's capabilities. To completely dismantle a terrorist group in the long term, counterterrorism activities should seek to dismantle a group's organizational tools. To prevent a particular attack or to alleviate an immediate threat, a group's operational tools should be targeted.

Groups of the Al Qaeda brand have shown the ability to evolve when faced with countermeasures by state authorities, changes in support from other states or militant groups, or shifts in popular support. However, terrorist groups in transition face difficult choices about their organizational structure, strategy, and tactics. Understanding the pressure at work on a group may help counterterrorism authorities apply measures that increase the chances of terrorists making bad decisions and mistakes.

What are the Challenges and Problems for Intelligence?

Effective counterterrorism requires good intelligence, but counterterrorism intelligence differs in many ways from the intelligence support that was needed during the Cold War and for which intelligence services remain in large measure organized. The major challenges and problems for intelligence reside with human and signals intelligence collection, analysis, cooperation with law enforcement agencies, and the sharing of intelligence – ensuring that real-time intelligence about terrorist activities reaches those who can most effectively counter it.

Counterterrorism intelligence is of three categories:

Strategic: intelligence about the organization of the terrorist organizations, leadership, intentions, aims, modus operandi, sources of funds, weapons and means at their disposal, and contacts with external elements, including foreign intelligence agencies.

Tactical: intelligence relating to specific plans of terrorist action, also called preventive and indications-and-warning intelligence, which would enable the state to preempt terrorist action, prevent attacks, and frustrate terrorist plans.

Psychological: intelligence covering details of psychological warfare propaganda of the terrorists and data relating to the terrorists, which enable the state to mount its own psychological warfare against them. Indicators of discontent against the leadership in terrorist organizations, coercive methods in the recruitment of volunteers, and misuse of children and women for terrorist operations are examples of such data.

While the coverage of strategic and psychological intelligence by the intelligence services in general has been satisfactory, the collection of tactical, preventive, and indications-and-warning intelligence has left much to be desired. This is due largely to the difficulties in penetrating terrorist organizations for collection of human intelligence and intercepting their communications for the collection of signals intelligence.

While strategic and psychological intelligence can be collected from open sources, peripheral secret sources, interrogation of captured or surrendered terrorists, and the analysis and exploitation of captured documents, IT hardware, and software, precise preventive and indications-and-warning intelligence can generally be obtained only from moles in key positions in the terrorist organizations and through interception of communications. Occasionally, such intelligence may also be forthcoming from captured or surrendered terrorists, their couriers, and so on, but such instances are rather rare.

Human Intelligence Collection

Counterterrorism is highly dependent upon human intelligence: the use of agents to acquire information and perform successful covert actions. Signals intelligence and imagery satellites have their uses in the counterterrorism mission, but counterterrorism intelligence depends much more on human intelligence collection. Though human intelligence collection is one of the least expensive intelligence disciplines, it can be the most difficult, and is undoubtedly the most dangerous for practitioners. Mistakes can be fatal, politically embarrassing, and undermine important policy goals.

There is a general belief that intelligence required for combating terrorism will require significant changes in the human intelligence collection effort. Terrorists do not usually appear on the diplomatic cocktail circuit or in gatherings of local businessmen. In many cases, they are also involved in various types of criminal activities on the margins of society. Terrorist groups may be composed almost wholly of members of one ethnic or religious group or family clan. They may routinely engage in human rights abuses. Developing contacts with such groups is obviously a problem for Western intelligence agencies. It requires long lead-time preparation and a willingness to do business with individuals sometimes of the most unsavory and corrupt kind. It cannot, in most cases, be undertaken by intelligence agents serving under official cover as diplomats or defense attachés. It requires in-depth knowledge of local dialects, customs, and culture. Much time and patience will be needed to train collectors in difficult skills and languages. Furthermore, the list of groups around the world that might at some point in the future be involved in terrorist activities is not short. Determining where to seek agents whose reporting will only be important under future eventualities is a difficult challenge, with the risk of needlessly involving the state with corrupt and ruthless individuals.

Penetration of terrorist organizations is an extremely difficult and also dangerous task. It is easier to penetrate the sensitive establishments of an adversary state than a terrorist organization. Moreover, it poses ethical problems that are not appreciated by public opinion. If an intelligence service plants a mole in a terrorist organization, its leadership would first ask him to carry out a killing or some other similar act to test the genuineness of his motivation and his adherence to the organization's cause. If the source comes back and asks his handling officer whether he should kill in order to establish his credibility in the eyes of the organization's leaders, the handling officer would be faced with a dilemma. He cannot tell his source: go and kill, so that we can prevent other killings in future. Setting a thief to catch a thief may be permissible for security agencies under certain circumstances, but committing a murder to catch a murderer is definitely not.

There are few other ways of penetration. One is by winning over and recruiting or by corrupting or blackmailing terrorists who are already accepted members of the terrorist organizations. Another way is a more indirect approach, through the channels of organized crime, which entertains relations with terrorist groups since it is an established fact that a number of Muslim terrorists have formerly been criminals, drug addicts, or alcoholics before their conversion to Islam and joining terrorist groups. To be able to successfully do this, the handling officer should preferably be from the same ethnic or religious group to which the targeted terrorist and his organization belong. Intelligence services often tend to avoid the recruitment of operational officers from the ethnic or religious group that has given rise to terrorism, and this gets in the way of penetration via winning over a terrorist already in the organization.

There cannot be a regular flow of human intelligence of the preventive or indications-and-warning type without the cooperation of the community to which the terrorists belong. Such cooperation is often not forthcoming, particularly with respect to Muslim terrorist organizations. Feelings of religious solidarity and fears of being perceived as betraying the cause of Islam by cooperating with the intelligence services come in the way of help from law-abiding members of the community.

There is a need for a series of policy decisions involved in a reorientation of human intelligence collection.

- A move towards greater reliance on nonofficial cover – meaning that agents are working as employees or owners of a local business and thus are removed from the support and protection of embassies that would be available if the agent had cover as a government official. If the agent must be seen as engaged in business, considerable time must be devoted to the "cover" occupation. Providing support, travel, pay, health care, and administrative services is much more difficult. The agent will not have diplomatic immunity and cannot be readily returned to his home state if apprehended in the host country. He may be subject to arrest, imprisonment, or, potentially, execution. Moreover, there is a potential for agents working in businesses to become entangled in unethical or illegal activities – to "go into business for themselves" – that could, if revealed, be highly controversial, embarrass their own government, and detract from the official mission.[179]
- Requirements for human intelligence collectors with highly developed skills in foreign languages are difficult to meet. Few graduates from colleges have such skills, and language education is expensive.

[179] The need to reorient the HUMINT collection effort to a greater reliance on nonofficial cover is discussed by Treverton, Gregory F, *Reshaping National Intelligence for an Age of Information* (New York: Cambridge University Press, 2001), 152–157.

Recruiting citizens who have ethnic backgrounds similar to members of the societies in which the terrorist groups operate may subject individuals to difficult pressures, especially if the agent has a family in the targeted area. Though there is a most pressing need for greater numbers of foreign-language capable intelligence personnel with fluency in specific and multiple languages, this lack of availability is the single greatest limitation in intelligence agency personnel expertise and a deficiency throughout most intelligence communities.

- It is administratively difficult to develop resources throughout the world over a long period of time, and costs are higher than adding intelligence staff to embassies. Few have predicted the intense concern with places like Somalia, the Balkans, Yemen, or Afghanistan that have recently developed. Ten years from now, there may be a whole set of challenges from groups that no one today is even aware of.

In short, reorienting human intelligence collection to give significantly greater attention to terrorist or potential terrorist groups would have important administrative implications for intelligence services. While budgetary increases would not necessarily be dramatic – even paying hundreds of human agents would be far less costly than deploying a satellite – the infrastructure needed to train and support numerous agents serving under nonofficial cover would grow significantly. Extensive redundancy would be required to cover terrorist groups that may never pose significant threats to Western interests.

A central issue for parliamentary oversight is the extent to which it and the public are prepared to accept the inherent risks involved in maintaining many agents with connections to terrorist groups. Unlike the situation in the Cold War years when some intelligence efforts were designed to be "deniable," it will be difficult for governments to avoid responsibility for major mistakes or ill-conceived efforts of their intelligence services, or for activities that, if revealed or leaked, could become highly controversial at home and abroad.

Signals Intelligence Collection

Penetration of terrorist communications is the other way of collecting precise preventive and indications-and-warning intelligence. In the past, terrorist groups relied mainly on couriers for communications. This made the penetration difficult unless the courier was caught and interrogated. However, the same technologies that facilitate globalization allow terrorist groups to communicate and operate on a global level. With the expansion in the area of operations and their external networking, terrorists have increasingly been resorting to modern means of

communications such as satellite and cellular phones, fax, and e-mail. The Internet in particular enables instantaneous communications between parent organizations and their distant and isolated terrorist cells. However, this makes them vulnerable to detection by intelligence services, provided they could break their codes and get some details of their communications drills.

High-tech capabilities will be required to influence this center of gravity. Due to the high volume of traffic on the Internet, singling out specific e-mails is problematic. Using commercially available cryptographic systems and encoding the message with one-time-pad systems would make it exceptionally difficult to detect terrorist communications. Add to these procedures those that call for frequent user identification changes or the technique called steganography, which buries messages in Web sites or pictures, and intercepting terrorist messages becomes nearly impossible.

The Internet is also being used to market the religious views or ideology of several terrorist groups. Web sites display information on how support can be provided or where to send money. Members can also log onto Web sites to obtain moral support for their cause and receive updates on world events and how they affect the overall effort. By maximizing the use of the Internet, either through Web sites or e-mail, terrorist organizations can reach a large number of people at very little cost. This is important, since most legitimate media outlets are usually denied to terrorist organizations.

One of the greatest effects of instantaneous communication provided by the Internet is the ability to maintain constant contact and situational awareness. As a result, key leaders remain constantly engaged and take command of the organization relatively easily. This diminishes the ability to influence terrorist group leadership.

However, terrorists continuously learn from their failures and keep changing their modus operandi in order to frustrate the efforts of the intelligence services to collect intelligence about them. The successful use of SIGINT and COMINT by the United States for the arrest of some senior operatives of Al Qaeda in Afghanistan and Pakistan during the last three years has made Muslim terrorists more cautious in the use of modern communication gadgetry such as satellite and mobile phones and adopt better communication security procedures. One can witness the results of this in Iraq.

Many successful counterterrorism operations all over the world could be attributed to successful communications interceptions. But even this is now becoming difficult, not only due to, for anyone who can afford it, the availability of sophisticated concealment, deception, and evasion technologies, but also due to the reluctance of political, judicial, and human rights organizations to admit the need for the updating of the laws and procedures relating to communications interceptions in order to

empower the intelligence and security agencies to deal with this new threat and to deny to the terrorists the benefits of these technologies.

Analysis

Actionable intelligence is essential for preventing acts of terrorism. The timely and thorough analysis and dissemination of information about terrorists and their activities will improve government's ability to disrupt and prevent terrorist acts and to provide useful warning to the private sector and the population.

Terrorist activities present intelligence analysts with major challenges. The prerequisite is an awareness of the social, ideological, and political environment in which terrorist movements develop. Such awareness requires detailed knowledge of geographic, ethnic, religious, economic, and political situations in obscure regions. There is no ready supply of analysts with command of such skills, except perhaps among recent emigrants who may have complex ties to their former homelands. And brand-new analysts sometimes take years to grow into mature and sophisticated analysts who see patterns, remember history, and know how to communicate well. Moreover, areas of concern are likely to shift over time. Thus, analysts could serve their whole careers without producing anything that the government really needs, and no good analyst wants to be buried in an inactive account with peripheral significance.

And there is the scarcity of needed language skills for translation, interpretation, and analysis, which is both a matter of quality and quantity. Technology, seen by some as the panacea for translation, is not highly regarded by real linguists or analysts who need high-quality translations. Language is an art as well as a science, and the current needs, with respect to terrorism, require an elusive mix of formal language, slang, codes, and multilingual capabilities. Al Qaeda, for example, contains many nonnative speakers of Arabic, poorly educated South Asians, and Muslims of very different countries; attention to perfect grammar is not the issue. And there remains the problem of how language-skilled employees and the broader regional knowledge they often possess is used in the intelligence process. Some elements of intelligence services know how to treat language officers as a vital part of the organization. In other parts of the intelligence community, language is more often considered a secondary skill, and is not valued sufficiently in recruitment or promotion of regional experts. Linguists should also not be physically separated from all-source analysts, and should be integrated to the maximum extent possible into the career development track of analysts.

In the case of the classical battlefield, knowledge of enemy capabilities is the focal point of interest at the tactical level, while knowledge of the enemy's intentions is paramount at the strategic level. The need for this knowledge has been translated into criteria and procedures aimed at producing essential elements of information, other intelligence requirements, and, more comprehensively and systematically, order of battle intelligence. With regard, in particular, to the imminence of aggression and the avoidance of surprise, indications-and-warning intelligence criteria and procedures have likewise been developed. These are not entirely or indiscriminately applicable to the counterterrorist effort. Nevertheless, from an intelligence perspective, if domestic as well as international terrorism is to be countered, it is precisely the capabilities and intentions of the various terrorist groups and their supporting networks that must be identified and dissected early on. The skillful adaptation – as opposed to the direct adoption – of time-tested classical intelligence methods, foremost indications-and-warning intelligence, constitutes and essential step in this direction.

What follows is a frame of reference for developing a specific set of indicators for terrorist threat assessment in terms of both terrorist strengths and weaknesses – in other words, indications-and-warning intelligence.[180] If properly adapted to the different geopolitical settings, it may serve as a substantive element in planning terrorist counteraction. Both components of terrorist counteraction – antiterrorism and counterterrorism – are predicated upon the collection, evaluation, and analysis of timely and accurate intelligence. Though this collection-evaluation-analysis process is the main task of intelligence services, it should also be conducted by other government agencies and the private sector to the degree and extent that defensive measures legitimately contribute to enhancing the security of the population and of corporate business.

- *Identify exploitable societal conditions*. These conditions are historical, political, economic, social, and religious. Terrorism does not develop in isolation, but feeds upon and exploits a wide variety of societal conditions present in a given community, country, or broader geographical area. Terrorist acts are in fact frequently conducted out of sympathy for causes extraneous to the venue where perpetrated – as demonstrated with the terrorist attacks in Nairobi, Dar-es-Salaam, and Bali, which had hardly anything to do with issues concerning Kenya, Tanzania, or Indonesia.

---

[180] Taken in adapted form from Pisano, Vittorfranco S, "Terrorism and Intelligence-and-Warning Intelligence," *Rivista di intelligence e di cultura professionale*, no. 12 (Servizio per le Informazioni e la Sicurezza Democratica: Roma, September–December 1998).

- *Determine the presence of one or more radical subculture*. While societal conditions strongly influence the birth and viability of domestic as well as transnational terrorist groups, particular attention should be devoted to a dominant factor: the presence of one or more radical subcultures. These draw their inspiration from well-defined or hazy ideologies corresponding to leftist, rightist, ethnic, theocratic, or mixed schools of thought. Subversive agitation is the offspring of a milieu directly traceable to a radical subculture.

- *Monitor subversive agitation, revolutionary publications and propaganda, as well as anti-institutional demonstrations and activities*. Because subversive agitation constitutes the operational cradle of terrorism, it is imperative that it be closely monitored. Subversive agitators typically recruit additional subversive cohorts, incite the population to disobey the laws, create civil disorder, and resort to street violence. Since groups of subversive agitators who have not reached the terrorist stage often coexist with ideologically kindred terrorist groups, the former can provide recruitment and support pools for the latter, thus reinforcing the terrorist ranks. In turn, the presence of subversive agitators belonging to different radical subcultures increases the potential emergence of terrorist groups with contrasting ideological or political orientations, thus producing more sources of terrorism.

- *Analyze terrorist ideological tracts and responsibility claims to identify ultimate goals and intermediate objectives*. Terrorist literary production, though often untruthful or based upon an ideologically biased perception of society, furnishes nonetheless valuable insights regarding the mindset, self-image, aims, and preferential targets of a given terrorist group. Terrorist manifestoes and declarations can also indirectly provide data to assess a given group's organization and capabilities.

- *Record systematically all terrorist incidents to establish modus operandi and to understand behaviors*. Modus operandi, whose sophistication varies according to group, includes recruitment, training, and employment of personnel; targeting (selective or indiscriminate); tactics (weaponry selection, ambushes, attacks, raids, abductions, hijackings, hostage taking); patterns (time element, coordination, target clusters, major and complementary actions); internal security and communications; logistics and finances, responsibility claims; and captivity rules. Modus operandi reflects both current and potential capabilities of specific groups. The fact that two or more groups issue from the same radical subculture is not necessarily indicative of shared operational methods and practices. Modus operandi is also

subject to modifications over time. Track and analyze group behaviors for early detection of potential threats.

- *Track technologies and technological innovations*. Closely follow the development of different types of technologies useable as components for manufacturing terrorist weapons, or which could be misused as weapons and explosives or to enhance the effects of terrorist attacks. Also track the development of new telecommunication technologies in order to get a better hold on terrorist interconnectivity and timely interception of communications.

- *Determine the structure of terrorist groups to assess capabilities*. Identify relationships by uncovering interactions and relationships between terrorist groups and their members, and link group members to understand formal and informal organizational structures. The structure is indicative of immediate as well as longer-term potential. Unicellular or multicellular and compartmentalized terrorist groups are rigidly or loosely structured, with centralized or decentralized leadership. In some cases, they can also serve as an umbrella for lesser aggregations. Militants are part-timers, full-timers, or mixed. In many cases terrorist groups reflect an ephemeral or ad hoc aggregation. Structure and size will affect not only security, discipline, training, command and control, communications, planning, operations, and logistics, but also a group's life span. Groups belonging to the same radical subculture do not necessarily, and in fact often do not, adopt the same structure.

- *Identify support organizations, movements, and networks*. Connect networks to expose connections between group members, other organizations, outside individuals, locations, facilities, and communication networks. These aggregations of external supporters facilitate terrorist propaganda, recruitment, logistics, and intelligence. Some of them are institution-based: in schools, factories, labor unions, unemployed societal strata, extraparliamentary political circles, refugee camps, immigrant communities, or extremist religious congregations. Others may be area-based, particularly where ethnic or separatist terrorism is active. In some cases, terrorist groups are flanked by political parties, usually extraparliamentary but with certain notable exceptions. Some groups are further supported by unlawful finance-gathering networks and charities totally dedicated to the terrorist cause.

- *Verify the presence of possible international linkages with kindred foreign groups and/or sponsor states*. Expose group operations by showing shared assets, materials, and supplies for carrying out terror-

ist missions. When present, these linkages are precarious, generally range from ideological solidarity to logistical cooperation, and occasionally entail operations. Nonetheless, they constitute a clear threat, since they broaden the terrorist support base and sphere of action. State sponsorship, which is a notable exception and not the rule, is more readily available to terrorist groups having a dual structure: an overt one for sociopolitical action and a covert one for terrorism itself. State sponsorship for subnational terrorist groups is generally self-serving and predicated upon plausible denial.

- *Probe exploitable terrorist structural and operational weaknesses and failures.* Assess vulnerabilities by evaluating funding resources, recruiting methods, communication networks, storage facilities, and other resources to uncover potential vulnerabilities. Terrorist groups thrive primarily on the elements of initiative and surprise, both of which are highly dependent upon clandestine structures and dynamics. At the same time, these groups are subject to constraints exploitable by counterterrorism agencies. The necessarily clandestine nature of terrorist aggregations is a double-edged sword. Living hidden requires discipline, commitment, and the ability to cope with stress. The application of security rules, particularly compartmentalization, must be constant: there is no room for exceptions or relaxation. Terrorist groups must also foreclose internal dissent and schisms. Likewise, the mood and reactions of supporters and sympathizers must always be gauged by the terrorist core. Indiscriminate recruitment can also constitute a fatal flaw. Personnel renewal is a challenge. Finally, failure to achieve its ultimate radical or revolutionary goal within the expected time frame can prove to be devastating to any terrorist group. Counterterrorist agencies must be prepared to exploit all of these factors.

- *Determine the type and extent of counterterrorism assistance available from the governments of allied and friendly states.* States often entertain different perceptions – accompanied by conflicting national interests and priorities – regarding the threat of terrorism and, more so, the adoption of suitable countermeasures. Unanimity or divergence of views among states contribute to strengthening or weakening the operational options of international and domestic terrorist groups as well as their respective supporters, particularly sponsor states. Concurrently, the absences of international or, at a minimum, regional consensus, seriously downgrade the options available to the counterterrorist agencies of single states.

Although conceptually sequential, the above outlined steps in practice usually require nearly concurrent application, particularly if multiple and separate actors account for subversive agitation, terrorism, or both. Moreover, it should not be forgotten that even after the emergence of terrorism, when prevention has obviously failed for political or technical reasons, indications-and-warning intelligence can still play a major role in the containment and repression phases of terrorist counteraction.

Once a terrorist group hostile to Western interests has been identified, the intelligence services will be called upon to focus closely upon its membership, plans, and activities. Many collection resources will be targeted at it and much of the information will be classified and highly sensitive. The terrorist target requires extraordinarily close attention to seemingly innocuous details, but it also demands big-picture thinking. Both require two different kinds of skills and analysts. One is the forensic work of piecing together minute fragments of information to make hypotheses about past events or potential planning. But the labor intensive, fine-grained work of developing databases on known or suspected terrorists is a job with little glory or reward. At the other end of the spectrum is the anticipation of the next moves or to imagine new scenarios for terrorist attacks. The most challenging problem for analysts at this point is to attempt to discern where the terrorists will strike and with what means. Open societies are inevitably vulnerable to terrorists, especially those terrorists willing to commit suicide in the process of seeking their goals. The skills necessary to anticipate the unpredictable are extremely rare. Thus, there is a need to bring the intelligence community's analysts together to do some longer-term thinking, scenario building, and estimative work. But the production of such work must have an audience. One of the reasons the strategic analysis of terrorism is declining is the greater value that senior customers place on more actionable or operational intelligence. Customers have to be willing to receive both tactical and strategic intelligence and to understand the difference between the two.

Some suggest a useful approach may be to assemble a special task force center, consisting of a number of analysts, to sift through all the available data. Such a counterterrorism center was created in the United States, to follow Al Qaeda, but did not foresee 9/11. The bottom line is that anticipating such attacks is intellectually difficult. Hiring more people and spending more money do not guarantee success. Moreover, expertise can even get in the way of anticipating a radical departure from the norm. Terrorists succeed by undertaking actions that are unprecedented or, to Western eyes, irrational. Thus, trained analysts with years of experience may be less inclined to "think outside the box" – al-

though ignorance of the terrorist group's composition and goals does not guarantee unique insights, either.[181]

Others suggest greater reliance on outside consultants or intelligence reservists when terrorist threats become imminent. Such an approach might also allow intelligence services to acquire temporarily the services of persons with obscure language skills. While there are security problems involved in bringing outside experts into a highly classified environment, this may be one approach that can provide needed personnel without unnecessarily expanding the number of government analysts.

Much of the information required to analyze terrorist environments derives from the extensive study of open-source documents – newspapers, journals, pamphlets, books, religious tracts, electronic media broadcasts, and so forth. Some believe that intelligence services overly emphasize sophisticated technical collection systems and lack a comprehensive strategy for collecting and exploiting such open-source information. Although efforts are clearly underway by all intelligence services to expand the use of open-source intelligence, many believe that the services should continue to concentrate on the collection and analysis of secret information. In this view, the intelligence services should not attempt to become a government center for research that could more effectively be undertaken by think tanks and academic institutions.

In regard to analysis, major issues for parliamentary oversight include holding intelligence services responsible for the quality of their work, the effective and efficient use of open-source information, and the appropriate use of outside consultants and academics. Analytical judgment is not easily mandated or acquired; leadership is primordial, along with accountability and a willingness to accept that even the best analysts cannot foresee all eventualities.

Intelligence and Law Enforcement Cooperation

Intelligence and law enforcement are becoming increasingly intertwined. Few doubt that valuable insights can derive from the close correlation of information from differing intelligence, security, or law enforcement sources. However, should the two communities draw too close together, there are well-founded concerns that either the law enforcement effort would become increasingly inclined to incorporate intelligence sources and methods, to the detriment of long-standing legal principles and constitutional rights or, alternately, that intelligence collection in-country or abroad would increasingly be hamstrung by regu-

[181] Betts, Richard K., "Fixing Intelligence," *Foreign Affairs* (January–February 2002):58.

lations and procedural requirements, to the detriment of national security.

But countering terrorism requires close cooperation between law enforcement and intelligence agencies. Some terrorists will need to be brought to justice in courts; others are dealt with by military forces or covert actions. In recent years, important steps have been taken to encourage closer cooperation between the two communities, but some believe terrorist acts may have been facilitated by poor information exchanges between intelligence services and law enforcement agencies and by blurred lines of organizational responsibility.

A recurring concern reflected in reports about activities of those involved in the 9/11 attacks has been the perception that information about the possible terrorist involvement of individuals may not be available to immigration, visa, border guards, and law enforcement officials who encounter the individuals. Sharing between all these critical interfaces was underdeveloped. There have not been centralized databases containing intelligence by which individual names could be checked. Although there are many potential concerns about the establishment of centralized databases, there is a need to ensure that law enforcement and other agencies, including those of regions and localities, have better access to information acquired by intelligence services about potential terrorist activities.[182] Investigating today's terrorist groups requires interagency communication and collaboration. It is essential that law enforcement agencies and task forces be able to collect and analyze data from multiple data sources in order to monitor, penetrate, infiltrate, disrupt, and prevent terrorist activity.

The bureaucratic response to shortcomings in sharing is usually to adjust training protocols, to develop job-swapping programs, and to have the leaders make symbolic gestures about the need for greater cooperation and collaboration across agencies. These steps are necessary but not sufficient. Collaboration is not instinctive in systems that are competitive, where incentives and rewards are structured within organizations and careers flourish most when talented staffers make themselves useful to their superiors and not by spending time in other agencies or ministries or making a priority of helping people across town. What is also needed is greater inculcation of civic values – of a belief that the success of others is a shared success, in service to the nation and its citizens. The reward system needs to recognize that the integration of information and policy knowledge so badly needed to defeat the terrorist threat is a newly important value.

---

[182] Krouse, William J. and Perl, Raphael F., *Terrorism: Automated Lookout Systems and Border Security: Options and Issues*. (Congressional Research Service: The Library of Congress, Report RL31019).

The relationship of intelligence collection to law enforcement in dealing with terrorism poses complex issues for policymakers. Terrorism can, of course, be attacked militarily without concern for domestic law enforcement, but most believe that such an approach is appropriate and practical only when terrorists directly threaten the state. In other cases, law enforcement may be the approach that can effectively deal with the problem while not undermining support for larger policy interests or leading to significant own casualties.

Information used in judicial proceedings is often of a different type than that usually collected by intelligence services. It is collected differently, stored differently, and must usually be shared to some extent with opposing attorneys. Nevertheless, in most countries, initiatives have been undertaken to enhance the usefulness of information collected by intelligence services to law enforcement agencies and vice versa.

Bringing law enforcement and intelligence closer together is not without challenges. The two sets of agencies have long-established roles and missions that are separate and based on constitutional and statutory principles. The danger of using intelligence methods as a routine law enforcement tool is matched by the danger of regularly using law enforcement agencies as instruments of foreign policy. Difficult decisions will have to be made, some affecting organizational responsibilities, and fine lines will have to be drawn. Bureaucratic overlap and conflicting roles and missions are not unknown in many government organizations, but such duplication is viewed with great concern when it affects agencies with power to arrest and charge individuals or to affect the security of the country.

But even if statutes and policies encourage closer cooperation between intelligence and law enforcement agencies, there will be other bureaucratic obstacles to be overcome. Within the intelligence community, there has been a tendency to retain information within the services or to establish special compartments to restrict dissemination for security reasons. Similar tendencies exist among law enforcement agencies that guard information necessary for their particular prosecutions. But channels for transferring information must be clearly established, and close encouragement and oversight by both the executive branch and parliamentary oversight committees is required to ensure a smooth functioning of transfer arrangements.

A key issue is the overall direction of the effort. Law enforcement may require that some information be closely held and not shared outside the organization or the ministry, but if law enforcement and intelligence efforts are to work more closely in dealing with international terrorist threats, procedures will have to be in place to ensure that important information is shared. However, a seamless system encompassing all echelons of intelligence and law enforcement agencies for storing

and exchanging information in real time on potential terrorist threats has yet to be developed.

Is There a Need for a New Approach to Intelligence?

Public debate over the U.S. government's responsibility for failing to prevent the 9/11 attacks has focused on the performance of U.S. intelligence and law enforcement institutions. There is a widespread perception that these agencies were organized and managed in ways that inhibited the flow of information and the proactive behavior that could have prevented the attacks. Few seem to be reconciled to the notion that 9/11 might not have been preventable. As always in Western democracies, such events regularly produce three responses:[183] (1) hot-tempered and hastily written allegations of intelligence failure, (2) postmortem studies of the intelligence record by groups inside and outside government, and (3) follow-up official commissions advocating far-reaching reorganization of the intelligence apparatus. Of these, only the postmortems are certain to be useful. Reorganization suggested by follow-up official commissions never seems to eliminate subsequent intelligence shortfalls. And finger-pointing has a singularly unproductive history. Although the mission and focus of intelligence is regularly revisited, innumerable reorganizations later, intelligence has still not been "fixed" to the satisfaction of all. If there is blame to assign, it must be shared by the intelligence community and those who have had a hand in reforming it.

The fact is that failures there have been and failures there will be. No intelligence agency in the world, whatever its human and material resources and its technological and human collection capability, can claim or hope to achieve omniscience. Intelligence services were never all-knowing, even with respect to conventional state adversaries. They cannot be expected to be all-knowing with respect to evolving, self-organizing networks of nonstate terrorist adversaries. The resulting gap has to be made good by better analysis and utilization of the available intelligence – however sparse it may be – and better coordination amongst different agencies of the intelligence community, better physical security, and better international cooperation. Many breaches of national security occurred in the past and continue to occur today, not for want of intelligence, but due to poor analysis of the available intelligence and inadequate follow-up coordination and action.

---

[183] Harris, James W., "Building Leverage in the Long War," *Policy Analysis* 439 (16 May 2002).

Intelligence services themselves are conscious of their inadequacies and of the gaps in their knowledge. They are making unpublicized efforts to improve their capability and performance. Better human agents, with language skills and knowledge of the cultures of their nonstate adversaries, are being recruited. Better training methods are being used, with the intelligence services of different countries helping one another in producing better trained operators and analysts.

Intelligence is a critical and early input into the government's ability to work the terrorist problem. But it is a contributing factor, and not necessarily the determining factor, in the government's success. Intelligence is more often than not policy-neutral information, and the intelligence collected can lend itself to multiple policy outcomes. Moreover, intelligence is all too often an invisible piece of policymaking, and the top of the executive branch rarely acknowledges to what extent decisions or actions were based on intelligence.

Intelligence collection and analysis, physical security, and crisis management are the three important components of counterterrorism management. If the intelligence machinery fails to provide early warning about an act of terrorism, the physical security apparatus should be effective enough to thwart the terrorists in their attempts to engage in terrorism even without advance warning. In the event of both the intelligence and the physical security mechanisms failing, the crisis management infrastructure should be able to cope with the consequences. On 9/11, while the intelligence and physical security apparatus failed, the crisis management machinery performed commendably, and did not let itself become paralyzed into inaction by the trauma of the terrorist strikes.

Intelligence remains the first line of defense and the critical element in combating terrorism. However, the adaptable nature of the adversary demands an equally agile intelligence effort. This will require changes in the intelligence field, going far beyond redrawing the organizational chart of intelligence and redesigning its chain of command. Thus, if there is a need for new approaches to intelligence, this is to be found in at least eight domains or processes: breaking down outdated barriers, fostering individual initiative, bolstering and opening analysis, improving intercourse between analysis and collection, strengthening counterintelligence, promoting research collaboration and better use of technological innovation, establishing metrics for measuring progress, and improving international intelligence sharing and cooperation.

Breaking Down Outdated Barriers

There is a need to counter the adaptable adversary with our own adaptation. Hierarchies are handicapped when confronted by flexible, highly adaptable, and networked enemies; thus they must be flattened. Intelligence communities remain hampered by internal barriers and walls meant to protect intelligence sources and methods—this at a time when the outside world sees great value in making unprecedented investments in getting interconnected. There is no clearer manifestation of stifling hierarchy than intelligence community "stovepipes" – barriers to lateral collaboration by restricting communications and rewarding only bureaucratic loyalty within the organization. This approach makes it possible for unrelated intelligence components in different institutions to do essentially the same work against terrorist targets, wasting resources and preventing many professionals from leveraging the efforts of counterparts who remain outside their immediate circle. The "need-to-know" principle, of course, cannot be jettisoned entirely, but the trade-off between protecting security and promoting collegiality certainly bears recalibration. Hierarchy and stovepipes prevent too many of the people working against terrorist targets from effectively communicating with one another. At times, these barriers even prevent organizations from becoming aware of one another's existence. Moreover, intelligence components working against terrorist targets should not be forced to deal with a maze of bureaucratic and security-derived obstacles. And there is the question of the relevance of classification and definitions devised long ago, which no longer fully correspond to the new types of threats.

Fostering Individual Initiative

The successful intelligence enterprise can become sufficiently agile if, like the terrorist network, it is driven largely by individual initiative rather than commanded entirely from the top. For this, senior intelligence leaders need to engage in creative delegation and promote initiative and creative thinking by the workforce, and, thus, have to break radically with the past tradition of striving to be the authors of new initiatives, rather than their enablers. Instead, they have to devote more time to challenge those managers and analysts ambitiously climbing the ranks, who have become so used to avoiding risks that would take them off the fast track. This tendency to confine risk taking to the top and to constrain individual initiative because it might lead to mistakes must change if the fight against terrorism is to succeed. An additional reason for empowering individuals is the efficiency gains produced by reducing the multiple layers of supervision designed to provide redundancy in an

effort to avoid mistakes. Economies can be realized by placing the individual analyst closer to the end-users of the product and relying more on individual accountability to ensure quality. In order to achieve such a change, intelligence services need to adopt a more risk-taking and failure-tolerant management approach.

Bolstering and Opening Analysis

More creative approaches to analysis are needed, and multidisciplinary analysis must be strengthened. Unlike traditional intelligence, where analysts are recruited right out of school and "grown" over time, intelligence needs to hire analysts at mid-career, after they have achieved a personal standing and complete fluency in – and at the expense of – the private sector. To handle secrets, the analyst must be an authority in his given area of expertise. Intelligence services should dispense with the idea that analysts should confine their attention to the dimensions of the terrorism problem that play to their "comparative advantage" of the collection intake – that is, secret information. All-source analysts can no longer rest their conclusions and their reputation on the 2 to 5 percent of the information from secret sources they deal with. In recent years, intelligence services have improved analysts' access to all of the resources made available by the information revolution. Thus today, when over 90 percent of the relevant information is readily available, analytic tradecraft – the truly superior ability to create value-added insights through superior analytical knowledge and techniques – has become a decisive element in the fight against terrorism.

The bureaucratic office, with analysts physically co-located with one another, must give way to virtual task forces comprised of the top individuals from different agencies, each having a personal reputation that is more important than their parent organization's reputation. Moreover, analysts fighting terrorism need to break down barriers to their ability to form alliances with external centers of expertise. For this, they need the ability to share data and analyses spontaneously. Informal peer-to-peer networks, creative alliances with think tanks, academic institutions, and other centers of expertise are a force multiplier. In addition, measures have to be taken to create and sustain "out-of-the-box" analytic approaches to difficult antiterrorism and counterterrorism issues, as well as to develop mechanisms to tap such expertise outside the intelligence community. Good academics invest considerable energy in finding out about the research efforts of their colleagues in other institutions. From similar efforts, analysts would reap dividends that at least match those of their academic counterparts. Thus, intelligence community business practices should promote rather than impede informal and

mutually beneficial contacts between analysts and the outside community. No organization can have a monopoly of expertise, especially on subjects as complex as the Islamic Reformation and terrorism. Only a vibrant, self-directed network with global reach will attract the bulk of the relevant information – hence, analysts and terrorist groupings will have to become magnets for relevant information from private sector peers.

The counterterrorism output from analysis must be based on research, conferences, and workshops; intake from informal networks; analytic gaming with red-teaming; advanced agent-based modeling and computer simulation; and collaboration across agencies and institutions. No approach should remain untested for its applicability to the counterterrorism problem. Processing matters must become a core competency in analysis. Moreover, only by establishing a digital network for collection, processing, exploitation, and dissemination can the full resources of various parts of the government, agencies, academics, corporations, and NGOs be brought to bear on topics such as terrorism and terrorism-connected crime. And only a connected community of analysts can know immediately where to find the specialized bit of expertise or the arcane fact that makes the difference in a piece of analysis or in a clandestine collection program.

Improving Intercourse Between Analysis and Collection

Combating terrorism will place intense pressure on all intelligence collection systems, and it may do so for a generation or more. While the collection of raw intelligence will remain critical, it will also remain insufficient against an adversary that is a dynamic, constantly evolving, and self-regulating force. No central authority within the network of terrorist organizations can control future operations, or has the responsibility for designing them. Thus, there is no triumph of intelligence collection that can completely remedy all of the intelligence shortfalls. But collection needs to be sharper and more focused on what counts rather than hopelessly broad. Improving the analytical component of counterterrorism and the intercourse with the collectors may be the most promising way to ensure that collection initiatives are well focused. Hence, steps have to be taken to sharpen the collection of raw intelligence by taking advantage of deeper analytical expertise, thus better focusing human intelligence, signals, imagery, and other collection systems. The issue is not exclusively the collection of tactical, preventive, and indications-and-warning intelligence, but also of enabling the counterterrorism community to tailor the long-term development of collection systems to targets. To achieve this, multidisciplinary intelligence analysts

and collectors can no longer function in largely separate electronic compartments, but need to build, entertain, and foster a permanent intercourse among one another.

Strengthening Counterintelligence

Counterintelligence becomes ever more important in combating terrorism. Particularly, operational counterintelligence and analytic specialization in denial and deception require greater emphasis. In the face of the information explosion and the globalization of transnational terrorism, the "needle in the haystack" problem in terms of anticipating terrorist threats and attacks becomes more difficult. Counterintelligence is one of four core competencies needed to protect intelligence from being misled. The other three are cultural intelligence specialization, denial and deception specialization, and the combination of global open-source benchmarking – essentially the art and science of pattern analysis from signals intelligence, which must be brought over to the open source world, both in print and broadcast media monitoring – with vastly improved processing to detect anomalies and patterns. Denial and deception consists of measures to counteract the efforts of the terrorist adversaries to escape detection by intelligence satellites, reconnaissance drones, signals intelligence, and other collection means, as well as measures to counteract adversary efforts to purposefully mislead intelligence services by generating data that point in the wrong direction. While the adaptable adversaries have the incentives and the means to deceive Western intelligence services, these cannot allow the terrorists to play games by placing false leads and producing false warnings.

Promoting Research Collaboration and Better Use of Technological Innovation

Investment in research and development and better use of technological innovation will undoubtedly bolster the position of intelligence services and expand their lead in counterterrorism capabilities. Particularly, innovations in intelligence collection and decision support, sensors, monitoring, and a greater emphasis on crosscultural communication will lead to a more effective response to international terrorism. So far, it seems that only the United States is willing and able to rigorously exploit the potentials offered by research collaboration and technological innovation. Other nations' intelligence services would be well advised to invest more in this area. Several tools, either on the drawing board or already implemented within the intelligence services of the United

States, will undergo great enhancements and refinements over the next years. How quickly they will mature or how vigorously they will be exploited cannot yet be known. Among the most promising innovations likely to emerge and having the greatest effect on winning the fight against terrorism are:[184]

- *Forward-looking intelligence*: The greatest value of intelligence – and the greatest challenge—is to anticipate terrorist actions and to translate that information into an effective response. Leaps in development will provide improved computer-based data fusion capabilities, modeling, and simulation to better understand possible scenarios and responses. Moreover, advanced language translation software is in development to better track terrorist communications.

- *Comprehensive space, air, land, and sea monitoring*: a network to monitor aircraft in flight already exists, as well as extensive tracking and imaging coverage of the earth from space satellites and selective monitoring of the land surface. Integration of current and new technology will lead to a global surveillance system that covers the sea as well as land and airspace. Such a capability will substantially improve security by monitoring vessels bound for Western waters, and will improve border and territorial surveillance and security.

- *Electronic tracking of money*: To a large part, terrorism is funded through complicated electronic transfers of funds. If such money is tagged electronically, it can be tracked worldwide to key operatives to effectively shut down a terrorist operation. New software and tagging technology is being developed that will not only strengthen global counterterrorism investigations, but also law enforcement efforts to bring organized criminal enterprises to justice.

- *Biological and chemical sensors*: The future of sensors may lie in the mimicry of nature, otherwise known as bio-mimetics. Imagine employing the sniffing capabilities of a beagle or the heat-seeking abilities of a viper to detect concealed bombs or weapons. The need for more accurate and timely detection of viral and bacterial pathogens will drive advancements in sensors, with the ultimate goal of combining chemical and biological threat detection into a suite of sensors. Advances in infrared, sonic, optic, and other types of imaging will provide innovative ways of long-range sensing and identification of

[184] See "Technology Forecasts. Battelle Panel's top ten innovations for the war on terror headed by technology advances to support better intelligence, decision-making." 2004 Press Release. At: http://www.battelle.org/forecasts/terror.stm.

threats in the air, water, or food supply. Sensors of the future will be deployed by highly mobile, reliable, and affordable robotics.

- *Technologies to neutralize explosive chemicals*: Many terrorist bombs today are improvised, made in homes and small laboratories using common chemicals, including ingredients in fertilizers. Terrorists can be denied the opportunity to gain the attention they want by creating, in essence, bombproof chemicals. A new generation of chemistry could neutralize the explosive compounds contained in these chemicals, rendering them unusable as bombs, even as research continues into emerging chemical threats.

- *Noninvasive and nondestructive imaging*: A new generation of X-rays is emerging to identify what is inside shipping containers, crates, trucks, luggage, handbags, sealed packages, and so forth. Such noninvasive imaging will provide a faster and more reliable level of security at harbors, airports, train and subway stations, and borders, and be commercially viable. A technology under development is terahertz radiation, or T-rays, that offer the potential of seeing the contents of closed containers without opening them or damaging contents. Great strides have also been made in using advanced technology for the identification of drugs and explosives.

- *Nonlethal directed energy*: In the arsenal of nonlethal weapons, the Vehicle Mounted Active Denial System (VMADS) offers much promise. Now in advanced development, VMADS uses high-powered directed energy that is capable of stopping people and machinery. It has the potential to interrupt a signal between a terrorist and a detonating device, or to set off land mines – all from remote location. The high-powered microwave also has potential law enforcement use, as the directed energy can be adjusted to focus on making a person's skin uncomfortably hot, while causing no dermal damage.

- *Twenty-first century public diplomacy*: The fight against terrorism is, in part, a war with extremists whose culture, worldview, and values conflict with those of the West. There are economic, religious, political, and ideological tensions between the Middle East and the West. Thus, tools for combating terrorism must include deploying mass communication to break down these barriers. What is needed is to project a more balanced image of Western culture through strategic, positive communication. This could be achieved by communicating the Western message through targeted use of mass media, developing a next-generation "Voice of America" approach, perhaps supported by the distribution of inexpensive, disposable televisions.

- *Distributed forces and an interlocking network*: This is military network-centricity taken to the smallest node. It will give the twenty-first century land warrior continual situational understanding while being a member of a widely distributed, noncontiguous force. Effective combat operations against terrorists and their allies require widely distributed armed forces. Enabling technologies such as advanced minicomputers and communication networks will turn these forces into distributed sensors as well as combatants, and allow them to provide information back to command headquarters. The forces are operated like a distributed information system with real-time awareness of the battlefield, giving commanders better data for decision making. Such technologies also will identify friend from foe in combat environments.

- *Encouraging public awareness and self-identification of terrorists*: The coming years will see innovative applications of behavioral science to combat terrorist activity. In some ways, terrorists operate like criminals, trying to behave secretively and inconspicuously and in the process, sometimes calling attention to themselves. To find criminals, law enforcement relies on a watchful public to provide tips. The worldwide information-saturated culture that we live in will expand further, creating new opportunities to engage the public to ferret out terrorists. A global "Amber Alert" system could be used to distribute multilingual information on known terrorists. A "Most Wanted" list could be tailored to help find terrorists hiding in plain sight. In addition, innovative methods will be deployed to coax terrorists into identifying themselves. For example, warning signs might be placed along a controlled access announcing that a security-screening checkpoint is coming up, just before a convenient opt-out or exit point. Anyone avoiding the checkpoint can be watched for further examples of self-incriminating behavior.

Establishing Metrics for Measuring Progress

Metrics will be needed for measuring progress in the counterterrorist effort, both on the results and the actions taken by intelligence. They should include measures of improved connectivity within the intelligence community, measures of the multidisciplinary approach of analysis and the structures that connect the community to the best and brightest outside the world of intelligence, and indicators of true analytic innovation and deepened expertise in outwitting the adversary. Any metric employed to gauge progress needs to make room for intelligent risk taking and failure tolerance. Intelligent risk taking and the

ability of individual initiative to overcome bureaucratic caution would be central themes in a successful counterterrorism effort.

Improving International Intelligence Sharing and Cooperation

International cooperation is taking place at the political and the professional levels, bilaterally and multilaterally. Networking at the level of intelligence professionals is more important than that at the political level. Professional networking has to occur at the multilateral as well as bilateral levels. The multilateral networking can take care of the development of appropriate concepts, processes, communications, and liaison arrangements; of coordination and use of technologies and databases; mutual legal assistance in dealing with terrorism; and training and other support. But sensitive operational cooperation will have to remain at the bilateral level and cannot be the subject of multilateral discussions, since leaks could come in the way of the effectiveness of such cooperation, which may involve ideas and concepts for joint operations to penetrate terrorist organizations in order to improve the quality of available human intelligence collection.

International intelligence cooperation has three aspects: making available technology, training, operational, support, and other facilities to one another; sharing of intelligence collected independently; and joint operations for the collection of intelligence through penetration and for neutralizing and disrupting terrorist organizations identified as common enemies.

While the sharing of technology, training, operational, support, and other facilities seems to have made satisfactory progress, intelligence sharing has yet to improve to the needed extent. Intelligence sharing provides a particularly significant lever and opportunity collectively to overcome obstacles, achieve quality control and consistency, to enhance responsiveness, and to create economies of scale and critical mass that would be difficult to attain if approached by individual nations. However, in a number of cases, sharing is still limited because of political, legal, and security concerns, and in some cases, legacy interests. Moreover, there are still lingering legacy organizational cultures that result in animosity and rivalry between intelligence services, between the services and law enforcement, communications voids, delayed or withheld intelligence, and breaches of the "third party rule." Furthermore, collective intelligence sharing is still too much limited by contrasts in processes and interests of intelligence collectors and law enforcement, European legal codes and English-based Common Law, and national regulations on the status and relations between the armed forces, police, and intelligence. Although there may also be organizational and political obsta-

cles on the supranational level, only NATO is in the position of a unique provider of deliverables in multilateral intelligence sharing. It is established, trusted, neutral, and proficient. It has political mechanisms for bringing matters forward. Unlike other international or regional organizations that would enter this field anew, it is cost-effective and does not have the reputation of squandering large amounts of funds without tangible results.

Joint intelligence operations have become much more numerous and have resulted in some successes. However, depending on the nations involved, there may still be considerable mental resistance to engage jointly in such ventures. Political and subjective factors such as "one nation's terrorist being another's freedom fighter" and "one nation's state sponsor of terrorism being another's strategic ally against terrorism" continue to come in the way of joint operations. As long as such mental resistance continues, international intelligence cooperation will remain halfhearted and only partially effective. The terrorists and their state sponsors will be the beneficiaries.

Reducing bureaucratic barriers, boosting multidisciplinary analysis, and rigorously improving interconnectivity and emphasis on individual initiative will remain prime strategies in the fight against terrorism.