1

Introduction

National-intelligence services, in the United States and elsewhere, had not digested the implications of the end of the Cold War when the first wave of terrorist attacks struck: September 11, 2001, in the United States; March 11, 2004, in Spain; and July 7, 2005, in Britain – dubbed "9/11," "3/11," and "7/7." They had not absorbed the effect of one major change when they were hit by yet another. Thus, intelligence is being reshaped under this onrush of events. Especially in the United States, it is also being reshaped under the looming shadow of acrimony about emotional issues at the edge of intelligence, issues with epithets like "Guantanamo" and "Abu Ghraib" and "torture." These epithets with their implications for intelligence are considered in Chapter 9. The onset of an age of terror has highlighted the role of intelligence services in detecting and preventing possible terrorist acts. At the same time, a series of investigations, especially in the United States and Britain, has focused attention on the performance of those intelligence services.[1] If and when the next major attack comes, recriminations about why it was not prevented will make the post–September 11 debate look decorous.

This book begins with where intelligence has been – the legacy of institutions and operating practices inherited from the Cold War – but its purpose is to describe where intelligence needs to go. The required reshaping is dramatic. In the United States, the process began with the Terrorism Prevention and Intelligence Reform Act of 2004; however, that law was the bare beginning of the reshaping, hardly the end. It is intriguing that all the countries that took intelligence seriously during the Cold War face some version of the same challenges: they have

Table 1.1. *Intelligence: From the Cold War to an Age of Terror*

	Old: Cold War	**New: Age of Terror**
Target	States, primarily the Soviet Union	Transnational actors, also some states
"Boundedness"	Relatively bounded: Soviet Union ponderous	Much less bounded: terrorists patient but new groups and attack modes
"Story" about Target	Story: states are geographic, hierarchical, bureaucratic	Not much story: nonstates come in many sizes and shapes
Information	Too little: dominated by secret sources	Too much: broader range of sources, although secrets still matter
Interaction with Target	Relatively little: Soviet Union would do what it would do	Intense: terrorists as the ultimate asymmetric threat

considerable capacity but a capacity that is primarily military in character, so they are asking how that capacity should be reshaped. In an age of terror, they all face the need to collect more information about their inhabitants: How can they do so without trampling on privacy and civil liberties? The challenges vary in scope and circumstances, but they are kindred across countries. This book draws comparisons across nations to illuminate issues, especially arrangements for domestic intelligence.

With the end of the Cold War and, a decade later, the onset of Muslim extremist terrorism, the task of intelligence changed dramatically. Table 1.1 summarizes the major differences.

These changes frame all subsequent chapters, with a number of themes common throughout. One theme is risk. Intelligence always has been a hedge against risk but now, as the nature of the threat has changed, so has the nature of the risk. Terrorists who are willing to die for their cause as suicide bombers, for example, cannot be deterred from acting in any way similar to the way that states could. Thus, there is even more pressure on intelligence, which now has to be not merely good enough to structure deterrent threats. Rather, it also needs to reach deeply into small groups – their proclivities and capabilities – to provide an understanding that can lead to preventive action. As the Irish Republican Army (IRA) stated after that group's bombing

of a Brighton hotel in 1984 failed to kill Prime Minister Margaret Thatcher, "Today we were unlucky, but remember we only have to be lucky once. You will have to be lucky always."[2]

A second theme is the corresponding expansion in the consumers of intelligence. National intelligence used to be designed primarily for a relatively small set of political and military leaders of states. Now, in principle, it could be of use to a huge number of consumers, from police officers on the beat to private-sector managers of major infrastructure. Intelligence has moved, according to the catchphrase, from the "need to know" to the "need to share" – a catchphrase that captures the diagnosis but badly poses the remedy.

A third theme is the increased number of needs for – and, therefore, types of – intelligence across a variety of time horizons from immediate warning to longer term understanding. Much of the Cold War intelligence was puzzle-solving, looking for additional pieces to fill out a mosaic of understanding whose broad shape was a given.[3] Those puzzles – for example, "How many warheads does a Soviet missile carry?" – could be solved with certainty if we only had access to information that, in principle, was available. Puzzle-solving is inductive. Mysteries are different; no evidence can settle them definitively because they are typically about people, not things. They are contingent; that is, mystery-framing is deductive – the analysis begins where the evidence ends.

There were mysteries during the Cold War, but the age of terror seems especially rife with them. For instance, many of another nation's military capabilities could be treated as a puzzle during the Cold War and assessed by counting tanks, divisions, and rockets. Now, however, even the capabilities of terrorists are a mystery: those capabilities *depend*, not least, on us. Given the lethality of even a single suicide bomber, what can be counted is not of much use to count.

A final overarching theme is boundaries – of both law and organization. During the Cold War, democratic societies drew boundaries – with varying degrees of sharpness – between intelligence and law enforcement, between home and abroad, and between public and private. The first two boundaries, in particular, were drawn to protect the privacy and civil liberties of a nation's citizens. In the circumstances of the Cold War, those boundaries made sense. However, they set up nations to fail against a terrorist foe who respects none of those

boundaries. Now, the balance between security and privacy is being struck anew and, in the process, the organizational distinctions – such as between intelligence and law enforcement – are being erased.

CHANGED TARGETS AND A MISMATCHED LEGACY

As an intelligence challenge, transnational targets such as terrorists differ from traditional state targets in a number of ways, which are summarized in Table 1.1. Chapter 2 describes the shift in more detail. Transnational targets are not new; intelligence has long been active against organized crime and drug traffickers but as a secondary activity. Although state targets of intelligence will remain – Iran, North Korea, China, and Russia, for example – the shift to terrorists as a primary target is momentous. First, while the current Islamic extremist terrorists hardly act quickly but instead carefully plan their attacks over years, transnational targets are less bounded than state-centric targets. There will be discontinuities in targets and attack modes, and new groups will emerge unpredictably.

Second, intelligence ultimately is storytelling. It is helping policy makers build or adjust stories in light of new or additional information or arguments. However, the new transnational targets deprive both intelligence and policy of a shared story that would facilitate analysis and communication. We knew what states were like, even very different states such as the Soviet Union: they were geographical, hierarchical, and bureaucratic. There is no comparable story for nonstates, which come in many sizes and shapes.

Third, given that U.S. foes were closed societies, Cold War intelligence (including analysis) gave pride of place to secrets – that is, information gathered by human and technical means that intelligence "owned." Terrorists are hardly open, but an avalanche of open data is relevant to them: witness the September 11 hijackers whose real addresses were available in California motor-vehicle records. During the Cold War, the problem was too little information; now, the problem is too much. Then, intelligence's secrets were deemed reliable; now, the torrents on the Web are a stew of fact, fancy, and disinformation.

Finally, and perhaps most portentous, terrorists shape themselves around us; that was hardly the case for the Soviet Union. As former

U.S. Secretary of Defense Harold Brown quipped about the U.S.–Soviet nuclear competition, "When we build, they build. When we cut, they build."[4] Although various countries – especially the United States – hoped that their policies would influence Moscow, as a first approximation, intelligence analysts could presume that they would not. The Soviet Union would do what it would do. The challenge, in the first instance, was figuring out its likely course, not calibrating the influence that other nations might have over that course.

The terrorist target, however, is utterly different. It is the ultimate asymmetric threat, shaping its capabilities to our vulnerabilities. The September 11 suicide bombers did not come up with their attack plan because they were airline buffs. They knew that fuel-filled jets in flight were a vulnerable asset, that defensive passenger-clearance procedures were weak, and that the scheme obviated the need to face a more effective defense against procuring or importing ordnance. By the same token, the London, Madrid, and other bombers conducted sufficient tactical reconnaissance to shape their plans to the vulnerabilities of their targets. To a great extent, we shape the threat to us; it reflects our vulnerable assets and weak defenses. As military planners would state, it is impossible to understand red – that is, potential foes – without knowing a lot about blue – ourselves – that is, our own proclivities and vulnerabilities.

That fact has awkward implications for intelligence, especially foreign intelligence that in many countries has been enjoined from examining the home front and, less formally, has worried that getting too close to "policy" is to risk becoming politicized. Moreover, to the extent that intelligence now becomes the net assessment of red against blue, that too has been the province of the military, not civilian, agencies.

The Cold War legacy of intelligence is mismatched to the changed threat. That legacy, the subject of Chapter 3, consists of three parts. The first is the boundaries that were drawn. In an important sense, it should not be surprising that cooperation between the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) before September 11 was ragged at best. Americans wanted it that way. Out of concern for civil liberties, they decided that the two agencies should not be too close. The FBI and the CIA sit astride the fundamental boundaries of the Cold War – boundaries between

intelligence and law enforcement, between foreign and domestic, and between public and private. The distinctions run deep. The boundaries were reinforced by the second legacy: the institutional legacy.

The institutional legacy, on the collection side, was an organization of "stovepipes" by source. The clandestine service, or directorate of operations, of the CIA was primarily responsible for espionage, or human intelligence (HUMINT); the National Security Agency (NSA) for signals intelligence (SIGINT); and the National Geospatial Intelligence Agency (NGA) for pictures and other imagery intelligence (IMINT). There was, perhaps, a certain logic to that organization during the Cold War. With one overwhelming target – the Soviet Union – the various "INTs" were asked, in effect, what they could contribute to understanding the puzzle of the Soviet Union.

For its part, analysis was organized primarily by agency, not by issue or problem. The directorate of intelligence of the CIA was first among equals, but the Defense Intelligence Agency (DIA) was just as large in numbers, and the much smaller State Department Bureau of Intelligence and Research (INR) tended to punch well above its weight in interagency discussions. The military services each had their own intelligence arm, primarily addressing the foreign threats that their service's weaponry would confront; the joint combatant commands also had their intelligence units, heavily tactical in orientation. In Washington, there were smaller analytic units in departments ranging from Energy to Commerce, which were explicitly departmental, serving the needs of local consumers.

If organizing intelligence by source on the collection side and by agency on the analysis side made a certain sense during the Cold War, it cannot be the right way to organize now. On the collection side, if the terrorist target is more of a mystery than a puzzle, then the Cold War's implicit competition among the INTs for puzzle pieces needs to give way to explicit cooperation across those INTs in framing the mysteries. Now, moreover, it is not just that there are more targets but also more consumers and more information – although the information is varied in reliability and little of it is owned by intelligence as were the secret sources during the Cold War.

The final Cold War legacy was a product of the boundaries. Domestic intelligence was a stepchild in the system. Unlike most of its major

partners, the United States had not created a domestic-intelligence service. Rather, the domestic-intelligence function, performed by the FBI, was twice circumscribed. First, it was part of the FBI, which first and foremost was a law enforcement organization. Understanding the Cold War FBI through its intelligence function, I realized after September 11, was like trying to understand the National Football League by interviewing the place-kickers. Intelligence may have been important but it was not central. Second, the domestic-intelligence function was limited by the boundary between intelligence and law enforcement, a "wall" that extended inside the FBI and inhibited cooperation among intelligence and law enforcement officials working on similar issues.

THE IMPERATIVE OF CHANGE

If the boundaries served the democratic nations tolerably well during the Cold War – in particular, by safeguarding the privacy of citizens – they set up those nations to fail in an age of terror. The imperative of change is the subject of Chapter 4. Terrorists respected none of those boundaries. They were not "over there"; rather, they were both there and here. Indeed, what is striking now is the contrast between Britain and the United States, countries usually considered as very close. However, for Britain, the terrorist threat had become almost entirely "domestic" by the mid-2000s, as the 2005 and 2007 attacks on that country demonstrated. The threat resided at home – although with tentacles reaching abroad, to Pakistan in particular. By contrast, for the United States, the problem is still primarily "over there," although with tendrils reaching into this country. Terrorists target not armies but rather private citizens. Although they might commit crimes, they might commit only one – and then it is too late; they cannot be treated as either an intelligence or a law enforcement problem but rather as both.

The effect of all these boundaries was vividly on display in the run-up to September 11. By the spring of 2000, two of the hijackers, al-Mihdhar and al-Hazmi, were each living under their own name in San Diego, and the latter even applied for a new visa. The Immigration and Naturalization Service (INS) had no reason to be concerned

because the CIA had withheld their names from TIPOFF, the basic terrorist watch list. Neither did the FBI have any reason to look for them – for instance, by conducting a basic Internet search for their names or by querying its informants in Southern California – because the last the FBI knew from the CIA was that the two terrorists were overseas. No agency told the Federal Aviation Administration (FAA) to be looking for the two, apparently because the FAA was not in the law enforcement business. The airlines were not informed because they were private, not public. So, on the morning of September 11, four sets of terrorists succeeded in boarding U.S. commercial jetliners, and three managed to strike their target: the World Trade Center towers in Manhattan and the Pentagon in the nation's capital.

In the United States, the 2004 Act made a start at reshaping intelligence. The Act – and more so the Senate version of the bill that was modified in conference with the House of Representatives – proposed national intelligence centers under the authority of the new Director of National Intelligence (DNI) and organized around issues or missions. The centers, with the National Counterterrorism Center (NCTC) as the prototype, would both deploy and use the information, technology, and staff resources of the existing agencies: the CIA, DIA, NSA, and others. They would be intelligence's version of the military's "unified combatant commands" and would look to the agencies to acquire the technological systems, train the people, and execute the operations planned by the national intelligence centers. So far, in addition to the NCTC, the National Counterproliferation Center is the only other center to be established, although the DNI has named "mission" managers for North Korea, Iran, and Cuba–Venezuela.

The FBI, under Director Robert Mueller, was facing enormous pressure, and there was considerable talk of creating a new domestic-intelligence agency separate from the Bureau. Mueller, however, moved rapidly to turn the Bureau from almost pure concentration on law enforcement to prevention and intelligence. Both Congress and the postmortem commissions decided to give the FBI time to see if the change could be made enduring. The FBI adopted the Weapons of Mass Destruction (WMD) Commission's recommendation to create not only a Directorate of Intelligence (DI) within the FBI but also a National Security Branch (NSB), incorporating intelligence and

the FBI's Counterterrorism Division (CTD) and Counterintelligence Division (CD).

Yet, the 2004 Act marked only the beginning of the change; Chapter 5 lays out the agenda ahead. The main challenge is also the reason for having a DNI in the first place – to better manage the entire set of U.S. intelligence agencies so that the nation gets the most from the $40-plus billion it spends annually on intelligence. John Negroponte, the first DNI, took over control of managing and delivering the "crown-jewel" analysis – the President's Daily Brief (PDB) – which had been the CIA's product. However, the nation did not need a DNI to deliver the PDB; for that, the former Director of Central Intelligence (DCI) was fine.

Rather, the DNI needs to be a major player in programmatic decisions – of which there was not much evidence in the DNI's first several years – a need more pressing as the distinction between "national" and "tactical" systems blurs, meaning that the intelligence agencies and the Pentagon share systems and compete for priority. This will require a much greater analytic capacity than what the DNI inherited if he is to be compelling inside the executive branch and with Congress.

At present, U.S. collection produces too much data and too little information, and the strategic-management task requires driving trade-offs not only across the stovepipes but also within them. U.S. collection techniques, especially for imagery, are fairly well understood by targets. Also, the Cold War espionage practices will not work against terrorist targets because, alas, Al Qaeda operatives do not go to embassy cocktail parties. The sheer volume of the data, or "take," from collection, just from intelligence's own secret sources, threatens to overwhelm the processing of it. The challenge is to be less passive and quicker in innovation. For signals, that means getting closer to targets. For imagery, it means smaller platforms, increased use of stealth, and employing more of the spectrum. For espionage, it means more diversity in spymasters and moving out of official cover. However, it also means being patient.

Meeting these challenges amounts to changing the agencies of the intelligence community to adaptive-learning organizations. The need applies with particular force to intelligence's most precious asset, its people. New recruits, across the community, are very different. They are fearless and computer-savvy – used to communicating, searching,

and reaching out. They will not tolerate the information environments – compartmentalized, slow, and source-driven – that current intelligence provides. Neither will they long be satisfied with work assignments that amount to, as one put it, "a few square miles of Iraq." They seek new challenges in "portfolio careers." To get and keep them – a great opportunity – intelligence will have to change the way it structures careers throughout the career cycle – from mentoring to lateral entry at senior levels. New personnel practices and new forms of training can also build jointness in a legacy of the stovepiped intelligence community. Training is similarly stovepiped and scattered; too much of it was oriented toward credentials rather than doing better on the job, and it was not integral to careers. There were no focal points for tool-building and lesson-learning. In all these respects, the DNI also has an opportunity.

The third major agenda item is domestic intelligence. If, thus far, the United States and its leaders have opted not to create a domestic-intelligence agency separate from law enforcement, the question of whether to do so will remain on the agenda. Another major terrorist attack would drive it immediately to the top. On this score, although international comparisons cannot settle the question for the United States, they are particularly apt because almost all of America's principal partners in the age of terror have chosen to separate domestic intelligence and law enforcement into distinct government agencies. For the United States, the choice is ultimately whether the considerable transition costs – costs driven home by the experience of the Department of Homeland Security (DHS) – are justified by potential improvements in domestic intelligence, especially in the value of what is collected and the value added by analysis.

A critical part of the agenda is intelligence analysis, the subject of Chapter 6. The postmortems in the United States, more so than in Britain, were scathing in regard to analysis – for instance, the WMD Commission on intelligence before the Iraq war: "This failure was in large part the result of analytical shortcomings; intelligence analysts were too wedded to their assumptions about Saddam's intentions."[5] The Senate Select Committee on Intelligence was equally scathing about the October 2002 National Intelligence Estimate (NIE), concluding: "Most of the major key judgments . . . either overstated, or were not supported by, the underlying intelligence reporting. A series