Control of a Terrorist Network: Lessons From the 9/11 Commission Report
Renate Mayntz

To link to this article: http://dx.doi.org/10.1080/10967490600899622

Taylor & Francis makes every effort to ensure the accuracy of all the information (the “Content”) contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at http://www.tandfonline.com/page/terms-and-conditions
CONTROL OF A TERRORIST NETWORK: LESSONS FROM THE 9/11 COMMISSION REPORT

RENATE MAYNTZ
MAX PLANCK INSTITUTE FOR THE STUDY OF SOCIETIES

ABSTRACT: The 567-page 9/11 Commission Report traces the actions of the Al Qaeda terrorists that led up to the 9/11 attacks on the World Trade Center and the Pentagon, and describes in detail the counter-terrorism activities of the organizations and offices in the American security community, focusing on the missed opportunities to prevent the attack. A careful analysis of the report permits us to identify the organizational, managerial, and cognitive preconditions of successful prevention. The analysis also shows that hard-to-control factors in the policy environment severely restrict the choice of prevention strategies. The pre-9/11 counter-terrorism measures of the U.S. were ill adapted to the special character of the threat posed by a transnational terrorist network.

THE REPORT

After the attacks on the World Trade Center and the Pentagon on September 11, 2001, two urgent questions were raised both in private and public discussions: why do they hate us so much to conceive of such a heinous deed, and why was it not prevented? The second question was asked most insistently by the families of 9/11 victims, and it was a group of them who formed an organization and pressured Congress to institute, against the wishes of the Bush administration, a commission examining in detail the history of the attack and what the competent American authorities had done and had failed to do in order to prevent it. The bipartisan National Commission on Terrorist Attacks upon the United States, called the “9/11 Commission” for short, embarked upon a sweeping investigation and produced a 567-page report that was published in 2004. The report traces the actions of the Al Qaeda terrorists that led up to the 9/11 attacks, and describes in detail the counter-terrorism activities of the various bodies and organizations in the American security community. Focusing on the missed opportunities to prevent the attacks, the report indirectly points out the conditions of effective control of terrorist organizations of the kind represented by Al Qaeda. Having previously studied, on
the basis of an extensive literature search, the organizational forms of both national and international terrorism (Mayntz 2004), I analyzed the results of the 9/11 Report in order to find out what we may learn from it about the preconditions, and the chances, of controlling a terrorist network. This requires a sort of backward reasoning: by identifying the deficits responsible for the failure of prevention, we can derive the factors that would make for successful prevention—but we can also recognize constraints and restrictions that are difficult to overcome.

The following observations are based on a single source, the 9/11 Report. Of the rich literature spawned by the event, I have only used two additional publications that cover the same subject (Posner 2003, Clarke 2004). Though more critical than the 9/11 Report, which deliberately uses a matter-of-fact approach, neither of these publications contradicts its findings in points that would be important for the following analysis.

**CONTROL STRATEGIES**

There are two basic approaches to control: law enforcement and prevention. Law enforcement, or the strategy to “discover and destroy” as the commission calls it, means to treat terrorists in the same way as criminals, and terrorist acts like criminal acts. Action is taken after the fact, by police forces (or the military). The “criminal” must be identified, in order to be hunted, caught, judged, and finally, sentenced. Law enforcement is a measure of last resort if prevention has failed. Prevention takes place “before the fact.” Legal rules backed up by the threat of sanctions presumably serve the purpose of prevention by making norm violation a costly risk. A general threat of sanctions attached to given categories of acts is, however, unable to prevent specific incidents, for instance of murder, robbery, embezzlement, or terrorism. Terrorists do behave rationally, but for many of them being caught, detained, or even killed are discounted costs; here the “Law” and available law enforcement measures have no preventive effect.

Prevention strategies can be either defensive, trying to protect the potential victim from attack, or offensive, trying to incapacitate the potential perpetrator—either directly by physically destroying him, or indirectly by making him unable to act and starving him out. There is a fluid boundary between these seemingly clear-cut categories. Border controls, for example, are both a defensive and an offensive measure: they protect the potential victim, but they also constrain the action space of terrorists. Promising control strategies of both types depend on the kind of threat. If the threat is a specific one, i.e., if it is possible to anticipate who might do what, where, and when, a feasible offensive strategy could be to detain the person or persons about to commit the act, and protection (sealing-off) of the threatened site would be a sensible defensive strategy. This strategy has been successful in the case of the so-called Millennium scare. Here at least the critical time was known (around New Year’s Eve), and certain sites such as computer centers and places of celebration appeared to be especially threatened. All agencies in the security community were on alert, and all threatened sites were highly protected. In the end, nothing
happened. One terrorist who planned to bomb the Los Angeles airport was caught when he tried to enter at the Canadian border.

The 9/11 attack was not a specific threat; when it happened, it came as a complete surprise to most—not so much with respect to the organization behind it, but with respect to the time, the place, and above all the kind of attack, i.e., by using hijacked civilian aircraft as missiles. If there is no credible lead as to the place, the time, the kind of a threat, and the identity of the potential terrorists, only highly general defensive measures such as rigid control over the movement of people, vehicles, and goods might serve. The extent to which such preventive measures are acceptable differs; in authoritarian regimes, potential troublemakers may be detained (or even murdered), but in a constitutional state with a legalistic culture, the actions of public authorities are constrained by law. The first condition of successful control is therefore to recognize the existence of, and identity of, a potential enemy. Such recognition may not permit us to anticipate specific terrorist acts, but it does permit us to develop a more pointed offensive strategy, i.e., to incapacitate the person, group, or organization presumably planning unspecified terrorist acts. This could either be done directly by physical destruction, or indirectly by cutting off their supplies and narrowing their action space.

### WHY PREVENTION FAILED: THE CHARGE

The 9/11 Report deals mainly with two basic prerequisites of successful prevention: information and the ability to act on it. The commission argues that, but for the deficits existing on both counts, 9/11 could have been prevented. Describing the organization and the operation of Al Qaeda, and reconstructing step by step what in the end led to the 9/11 attacks, the commission has identified a number of points where timely intervention might have incapacitated Al Qaeda, or could at least have prevented these specific attacks. The commission enumerates “late leads” that were not pursued, and lists actions by the CIA and FBI that might have made a difference but were not undertaken (National Commission 2004, 266–277, 355–356). At least two of the hijackers who had previously been identified as possible terrorists could, for instance, have been held for immigration violations, had they only been found in the U.S. “In sum, the domestic agencies never mobilized in response to the threat. They did not have direction, and they did not have a plan to institute. The borders were not hardened. Transportation systems were not fortified. Electronic surveillance was not targeted against a domestic threat. State and local law enforcement were not marshaled to augment the FBI’s efforts. The public was not warned.” (Ibid., 265) These failures, so the 9/11 Commission maintains, were largely the result of insufficient information and insufficient action capabilities, which in turn followed from the structure of what one could call the security community, from organizational features of the agencies involved, and from a faulty allocation of funds. Underlying this diagnosis of failure we can recognize a simple control model whose structure is similar to the basic three-step model of a policy process, moving from problem definition (i.e., information) via policy choice to
policy implementation (i.e., action). This basic model must be disaggregated (or differentiated), and specified for the particular kind of control task. Only then will it be possible to pinpoint conditions for the control of a terrorist network.

Let us begin by analyzing the charge of the 9/11 Commission in more detail. With respect to information, in the eyes of the commission the main cause of failure was not its absolute lack, but the way it was, or rather was not, processed. The organization Al Qaeda as such was known from the time when the U.S. helped to finance the war against the Soviets in Afghanistan; information on its goal and strategy had been supplied by Bin Laden himself. But it seems that there existed only little useful up-to-date information on the structure and action plans of Al Qaeda. Such information might be obtained from the interrogation of detainees, or from “moles” (“assets”) within, or close, to Al Qaeda. But in the case of 9/11, the capability of the U.S. to use such sources was obviously underdeveloped. The FBI lacked Arab-speaking officers who might have served as undercover agents, and there were not even enough competent translators, so that a huge backlog of un-translated intercepts in Arabic built up (Ibid., 77). To collect information that first permits us to identify the existence of an enemy, and subsequently to convert a perceived general threat into a specific threat that could be addressed by more pointed measures, is an obvious precondition of successful control.

All actors and agencies that are part of an existing control structure are permanently looking out for danger signals, for intelligence that requires them to become active. It is evident that the danger signals that were recognized before 9/11 did not add up in time to a correct assessment of the threat posed by the scheming of Bin Laden, and the strength of Al Qaeda. There were individuals within the American security community who, in the months before 9/11 when “the system was blinking red” (Ibid., 254), warned that an attack was imminent, that it was aimed at landmark targets, that airplanes could be involved, and that it could take place in the U.S. But these warnings were widely dispersed in the system. If, so the commission maintains, the bits and pieces of information about the behavior and movement of the future 9/11 pilots and operatives (the so-called “muscle men”) that was available at different places had been shared, and used among other things to tighten border controls, the 9/11 plan could have been disrupted. In the view of the commission, the crucial reason that this did not happen is insufficient information sharing: within agencies, between agencies, and upward to the political leadership.

With respect to the ability to act upon threat information, the commission mentions repeatedly a shortage of funds for organizational units specialized in anti-terrorism work, or for certain preventive measures that were considered. The fault, however, was in the allocation of funds rather than their objective availability, from the responsible congressional committees down to the individual agencies. Nor was it technically impossible to devise an integrated electronic data-base of visa, law enforcement, and watchlist information, or a monitoring system for foreigners entering the U.S. on a student visa. Aside from funds, it was the lack of intra- and inter-agency cooperation that delayed or blocked these measures. Whether judges refused a needed warrant, the military hesitated to deploy a drone, important files were seized but not passed on to a unit or agency that might use them, or CIA field offices
insisted on keeping a case to themselves: in all such cases lack of cooperation prevented timely action. The commission therefore finds the main cause of insufficient action capability in coordination deficits, a concept covering directive authority as well as horizontal cooperation.

**STRUCTURAL AND ORGANIZATIONAL CAUSES OF INFORMATION AND COORDINATION DEFICITS**

Projecting the commission’s analysis of the failure to prevent 9/11 upon the general control model referred to earlier, it appears that the deficits in sharing information and in coordination were caused by organizational shortcomings. The reform recommendations of the commission, at any rate, focus on agency organization, management, and authority, in addition to the allocation of funds. The implied causal argument is that a suitably organized (and funded) control structure permits the correct perception of a threat, which triggers the re-allocation of attention and the re-definition of priorities, which then leads to the mobilization of action capacities and to action. To assess whether organizational factors bear in fact the main responsibility for the failure to prevent 9/11, it is necessary to give at least a rough description of the U.S. control structure as it existed before the attack (National Commission 2004, 71–107, 407–408).

The set of agencies involved in some way with national security was roughly divided into two functionally defined communities, the law enforcement and the intelligence community, respectively. The law enforcement community included the criminal branch of the FBI, the INS, the Customs Service, local police, and the courts.

The FBI (Federal Bureau of Investigation) is an agency in the Justice Department, which also houses the U.S. Marshals Service and the Drug Enforcement Administration. The FBI has collected domestic intelligence since the 1930s. Responsibilities in connection with foreign and foreign-inspired subversion and espionage, with which Roosevelt charged the FBI, were transferred to the newly established CIA (Central Intelligence Agency) after World War II. The FBI has 56 field offices (or stations) in the U.S.; they set local priorities. According to the “office of origin system,” the station where a “case” originates remains responsible for it. The FBI has criminal as well as intelligence agents; following from a shared belief and ingrained practice rather than formal rules, information sharing between these different agents at the same level is quite limited (Ibid., 271). The FBI is used to write up witness interviews, but not to produce proper intelligence reports that summarize and assess information, and it complies with the norm not to disclose information relevant to a pending investigation. A singular exception to this practice was observed on the occasion of the Millennium scare, but afterwards the FBI “returned to its normal practice of withholding written reports” (Ibid., 180–186). The relationship between the FBI director and the U.S. president is “nearly nonexistent,” and information sharing with the rest of the national security community is insufficient (Ibid., 358).
The Immigration and Naturalization Service (INS) counted 9,000 border patrol agents at the time, 4,500 inspectors, and 2,000 special immigration agents. Its focus has long been on criminal aliens and illegal immigrants in the southwest of the U.S. Given the extended borders of the U.S. and the amount of cross-border traffic, this is judged insufficient. INS technology has long been outdated; efforts to automate a joint watchlist used at entry points and by consulates were made only in 1993. The effort to set up a system to monitor visa compliance of foreign students after entry failed.

The intelligence community included the CIA, intelligence agencies in the Defense Department, the intelligence part of the FBI, and a host of smaller units in the Departments of State, Treasury, Energy, and in the Coast Guard. The CIA is an independent agency established in 1947; it serves the president directly. It has stations abroad, and a Clandestine Service that needs approval from Washington for specific actions. Resources are centrally allocated. The CIA is an organization “institutionally averse to risk, with its capacity for covert action atrophied, predisposed to restrict the distribution of information, having difficulty assimilating new types of personnel, and accustomed to presenting descriptive reportage of the latest intelligence” (Ibid., 93). In the Cold War period, a paranoid fear of penetration by Soviet “moles” reinforced the tendency to compartmentalize and keep secret information (Ibid., 91). There is an ingrained rule that sources must be protected. From the information collected and put into intelligence reports, only a fraction goes into the President’s Daily Brief (PDB), which only a small circle of leaders gets to see; the Senior Executive Intelligence Brief and reports that are distributed more widely contain less information.

Among the other actors in the intelligence community, the Department of Defense is the most important. The intelligence agencies in Defense focus on military intelligence; Defense receives 80% of U.S. intelligence spending (Ibid., 86). One of the intelligence agencies in Defense is the National Security Agency (NSA), which, however, may not collect data on U.S. citizens without a warrant; its focus was therefore on foreign intelligence, and it is “almost obsessive” in the protection of sources (Ibid., 88).

This variegated intelligence community was supposedly led by a Director of Counterintelligence (DCI), but he lacked authority in personnel and budget matters and was unable to intervene into agency routines. The Counterintelligence Center created in the mid-1980s was explicitly charged with coordination functions. Staffed mainly by FBI officers, it never assumed an independent role, and remained ineffective.

This brief description of the control structure existing before 9/11 highlights several features responsible for the failure of prevention. There were barriers to information sharing, and dysfunctional routines and orientations. To some extent, these organizational features are the result of functional differentiation between agencies charged with different tasks. The intelligence community is responsible for discovering information relevant to national security; intelligence agencies generally tend to protect sources, and are afraid of counter-intelligence (“moles”). The frame within which different intelligence agencies seek information quite naturally differs between the CIA, concentrated on foreign intelligence, and the agencies in
Defense, which work within the framework of military policy. The agencies in the law enforcement community are bent on detection and punishment; they operate within a legalistic frame that constrains quick and independent action. Even in the later 1990s, “officials continued to think of terrorists as agents of states... or as domestic criminals” (Ibid., 108). From the perspective of fighting terrorism, these may be dysfunctional orientations and routines. But terrorism is only one among many security problems, and for many if not most agencies and field offices, illegal immigration, drugs, and “normal” crimes were more relevant threats than terrorism. Different tasks do require different orientations, and it would not be meaningful to commit all agencies in the security community only to counter-terrorism.

In the face of a high degree of organizational differentiation and specialization, coordination is indeed a crucial requirement. What is needed for control is a monitoring institution watching out for terrorist threats, and a leader who in case of need is able to mobilize the differentiated security community and coordinate its actions. In the case of 9/11, coordination was difficult because different agencies tended to defend their respective domains, hedge information and funds and had developed different organizational cultures, standards and routines. Thus the foreign-domestic divide within the intelligence community impeded the sharing and pooling of information. Structural barriers to cooperation within agencies were evident in the case of the FBI with its relatively autonomous field offices and its two functional branches. To overcome such barriers, a strong leadership able to give policy directions and enforce cooperation would have been needed. Leadership would also have been needed to identify required capabilities and to insist that they be developed, such as an up-to-date control technology (INS), or the capability to engage in covert action (CIA). But the management of counter-terrorism policy within the differentiated security community was highly divided, and the capacity to set priorities and to move resources weak. For this reason one of the main reform recommendations of the commission has been the creation of a new National Counterterrorism Center and a powerful National Intelligence Director, with full authority over budget and personnel decisions and direct access to the president. The commission also asked to unify congressional oversight in order to strengthen political support for anti-terrorism matters.

COGNITIVE CONTROL PREREQUISITES

Organizational shortcomings are in fact serious impediments to the successful control of a terrorist network. But as the commission itself has pointed out, most impediments to successful control can be overcome if a threat is clearly perceived, as it was in the case of the Millennium scare, when all agencies, setting routines temporarily aside, cooperated in the interest of a joint purpose. Though the reform proposals of the commission only address organizational questions, in chapter 11 of the report “imagination” is discussed as one of the factors that would have been necessary to prevent 9/11. In fact, threat perception is the basic condition of control. Sharing and pooling information become important once a threat is perceived; they do not automatically produce that perception.
Threat perception requires collecting information, but in order to know where to look, and what to look for, some idea as to the nature of the threat must already exist. Nor is threat perception an automatic result of sharing whatever information agents have; a general directive to share information would only produce unmanageable information overload. Criteria of selection are needed in order to recognize what bits of information could be used by whom. Productive information sharing therefore presupposes again what it is meant to produce, the perception of a possible threat. The same is true once more for the pooling of information, the construction of a more detailed image of a specific threat out of unconnected bits and pieces of information. To compose a puzzle out of many separate pieces is extremely difficult without a clear image of what the finished puzzle might look like. The inherent ambivalence of (most kinds of) intelligence is a problem that cannot be remedied by organizational reform and wider sharing of information. As a consequence of the recursive nature of the cognitive processes involved, there are serious limits to the effect that organization (in the narrow sense of formal structure) can have on threat perception.

The narrative in the 9/11 Report makes evident that the new nature of the threat posed by a transnational terrorist network like Al Qaeda was not recognized. Terrorists were perceived as criminals operating domestically, and law enforcement was the way to deal with criminals. This initial misperception made it difficult to recognize the salience of available bits of intelligence. Especially from the description of “missed opportunities,” “one can see how hard it is for the intelligence community to assemble enough of the puzzle pieces gathered by different agencies to make sense of them” (National Commission 2005, 355). “(N)o one working on these late leads in the summer of 2001 connected the case in his or her in-box to the threat reports agitating senior officials and being briefed to the president” (Ibid., 277). The Al Qaeda network itself was aware of an imminent attack (and of its several delays), and some of this intelligence seems to have seeped to U.S. agents. These, however, did not recognize the links between the people and the acts they knew about. The FBI did not collect intelligence on terrorism systematically, and “never completed an assessment of the overall terrorist threat to the U.S. homeland.” (Ibid., 77) Somewhere in the system there were puzzle pieces that would have spelled, if put together, the planned attack. All of the features of the 9/11 attack—that it took place in the U.S., that landmarks were the target, and that airplanes can be used as missiles—were anticipated as a real possibility by some lower level officer. They were not taken seriously because their warning did not fit the dominant view of the threat situation. And thus the information that was available, dispersed in the system, was not put together and did not amount to “actionable intelligence” (Ibid., 260).

To be believed, warnings must be credible. In spite of the fact that threat reporting intensified by July 2001, the FBI stated it had “no information indicating a credible threat of terrorist attack in the United States” (Ibid., 258). Doubts in the credibility of intelligence had already been a major obstacle in dealing with the attack on the American destroyer USS Cole in the port of Aden on October 12, 2000. Applying intelligence standards of proof in the assessment of available information, the CIA never stated with certainty that Bin Laden had been responsible for this terrorist
act. On a previous occasion, retaliatory air strikes against Libya seemed to have stopped Libyan state terrorism; this suggested an air strike in response to the attack on the USS Cole. But the lack of certainty with respect to the involvement of Bin Laden prevented Clinton from responding in this way. In the case of 9/11, President Bush’s Daily Brief (PDB) did say on one occasion that Bin Laden was determined to strike in the U.S., but “the threats received contained few specifics regarding time, place, method or target” (Ibid., 262–263). Thus the attack of 9/11 remained one—rather unlikely—possibility among many. The certification of intelligence is an important facet of the “information” component in the basic control model.

Threat perception is intimately linked to “learning,” because present situations tend to be interpreted in terms of past experience. In the case of qualitatively new threats, such learning is dysfunctional. The report contains many examples of dysfunctional learning. The attack on the USS Cole, the African embassy bombings in 1998, and the Rhiyad attack in 1995 seemed to indicate that targets tended to be non-U.S. Thus when 9/11 approached and “the system blinked red,” domestic threats did not appear very likely, and most preparatory action was taken overseas. Overseas stations were used to deal with terrorist threats and had action plans, while “domestic agencies did not have a game plan” and hence “did not perceive a call to action” (Ibid., 264). The size of the threat was underestimated because so far, relatively few people and even fewer Americans had been killed in terrorist attacks. In the 1993 bombing attack on the World Trade Center, there had been few casualties, and it was cleared up quickly. This incident “taught” people that foreign agents might commit terrorist acts in the U.S., but the lesson was erased by the fact that the 1995 Ohio bombing, which had at first been attributed to an Arab foreigner, was in fact committed by an American (Posner 2003, 90–101). While familiar with the hijacking of aircraft for purposes of extortion, the Pentagon, on the basis of the experience with Iran, was mainly concerned with the possibility of hostage-taking. Except for some isolated individuals believed to be raving, nobody imagined that hijacked aircraft would be used as missiles against U.S. landmark buildings. The Federal Aviation Administration in particular did not think the 9/11 kind of threat possible, and did not use the State Department’s watchlist for passenger prescreening. If airplanes were to be involved, an attack from outside the U.S. was considered much more likely.

Dysfunctional learning has also hampered the reaction capacity of U.S. control agents. Both the FBI and the CIA “learned” from the harsh criticism that some of its previous activities had met. Since the 1950s, the FBI collected unauthorized intelligence in investigating right- and left-wing U.S. suspects. In the early 1970s, this elicited public criticism, and in 1978, the Foreign Intelligence Surveillance Act was passed, which strictly regulated all action directed at foreign agents in the U.S. The FBI consequently retreated to strict legalism. The need to obtain a warrant, or court review, for many actions prevented the FBI in several instances from uncovering intelligence important to 9/11. The CIA in its turn had repeatedly planned, and actively engaged from the 1960s onward, in covert actions that were considered illegal. This again triggered a severe critique when these actions became public. After the Watergate era, Congress established oversight committees to assure that the CIA
did not undertake covert action contrary to U.S. law (National Commission 2004, 90). Henceforth, the CIA was wary not to infringe legal norms in its actions.

The perceived nature of the threat determines which agency will play the focal role in prevention; if the threat is misperceived, allocation of responsibility may also be wrong. In the 1960s and 1970s, the State Department managed counterterrorism policy, since terrorism threats were seen to emanate from foreign states. When Al Qaeda was recognized as a serious enemy, the CIA became the focal actor to confront it. Al Qaeda being a foreign-based organization believed to strike in other countries, the domestically oriented FBI played only a secondary role. Agencies in the Departments of Defense and of State were involved only episodically (Ibid., 400). This allocation of responsibility turned out to be inadequate in view of Al Qaeda’s activities within the U.S., and the support it had from its Afghan base.

Threat perception is the condition for the re-allocation of attention, and the re-definition of priorities. The less urgent the threat, the more likely will counterterrorism policy come up against the problem of overload. Every government has to operate permanently under an overload of problems and issues to attend to, and attention, always a scarce resource, will be devoted to the politically most pressing, or threatening ones. This holds both for foreign policy and for domestic policy. Before the “war on terrorism” became a top priority, counterterrorism had to compete with other legitimate policy goals. In the field of foreign policy, Iraq, North Korea, and the Israel/Palestine peace process commanded the attention of the U.S. government in the 1990s. The American Congress is oriented toward domestic affairs, and in the committees dealing with national security issues, terrorism was a second- or third-order priority (Ibid., 106). The Treasury, focused on drug money flows, paid little attention to the financing of terrorism. The initial refusal of the U.S. military to intervene in Afghanistan was motivated, among other things, by the priority to create 21st century armed forces (Ibid., 208).

The allocation of attention is partly a matter of structure. Thus, international terrorism “fell between the cracks” of the committee structure in the U.S. Congress (Ibid., 105); this, and the lack of a powerful and independent agency charged with counter-terrorism, militated against the early development of measures to contain Al Qaeda and prevent 9/11. But there were also other, situational factors that detracted from the development of such a policy. During the Clinton administration, the Lewinsky scandal commanded priority attention. Later, the imminent end of the legislative period dissuaded the outgoing administration from starting something big, and when Bush got into office, his administration had to get settled, make personnel decisions, and decide on priorities. It needed something like 9/11 to change political priorities drastically in favor of fighting terrorism.

**CONTROL MEASURES TAKEN AND NOT TAKEN**

Since no specific threat to domestic targets coming from Al Qaeda was perceived by the dominant actors before 9/11 actually occurred, it was not possible to take measures to prevent this particular attack, or more generally to prevent any major
terrorist attack against landmark targets in the U.S. Nevertheless, after the bombing of the American embassies which, in contrast to the attack on the USS Cole, had been explicitly linked to Bin Laden and Al Qaeda, in late 1997 a series of preventive measures were considered. These measures were directed against Bin Laden and Al Qaeda, as the originators of a threat that remained diffuse. A consideration of the measures chosen and not chosen, shelved or implemented, can point to additional conditions of successful control of a terrorist network beyond the organizational and cognitive factors already discussed.

The measures considered included some direct offensive measures, mainly directed at Bin Laden, who had finally been recognized as a dangerous individual. Attempts to capture Bin Laden and to bring him before an American court were planned, but never executed in the end. The same holds for plans to kill Bin Laden by an air strike against a camp in Afghanistan when he was known to be there; this, too, was never actively attempted. As the threat signals became stronger, military invention against the Taliban was briefly talked about, but never seriously considered. The only offensive actions actually undertaken were of a generally preventive nature, and aimed to cut off the vital resources of Al Qaeda.

The 9/11 Commission was well aware of the range of resources that a transnational terrorist organization needs and that might therefore be the target of preventive measures (Ibid., 172–173, 365–366). To maintain itself and to prepare and execute terrorist acts, a transnational terrorist organization needs mainly members, money, weapons, and a safe haven; members must also be able to communicate over wide distances, and in preparing attacks they must be able to move about freely. Only some of these resources were in fact targeted, and where attempts were made to constrain them or cut them off, the measures were taken only half-heartedly, came too late, or were ineffective.

There was, to begin with, no policy to impede the recruitment of new active members to Al Qaeda: this, in fact, is clearly beyond the power of agencies directly involved in counterterrorism. As the commission recognizes, it takes a very comprehensive, indirect, and long-term policy to combat the causes making membership in a given terrorist organization unattractive to potential recruits.

As for weapons, intelligence agencies generally try to prevent the acquisition of weapons of mass destruction by terrorists, but are incapable, especially in the U.S., of preventing firearms and dynamite from getting into their hands. However, in the case of 9/11 previously acquired weapons played practically no role. No attempt was made to prevent the use of hijacked aircraft as weapons, since no such use was expected.

Money was one resource in fact addressed, but too late to hurt, and not very effectively. U.S. authorities first froze assets of Bin Laden in the U.S., and later also of the Taliban, but this did not amount to much. Most of the Al Qaeda funds at this time came quite legally from charitable and welfare organizations that were at first sight beyond suspicion and/or resided and operated outside the U.S. Bin Laden himself had been cut off from his inheritance and had lost valuable assets in Sudan. There were also attempts to get major banks to look out for, and prevent, money laundering and suspicious transfers. The effectiveness of this approach was limited
by the independence of banks, and the fact that Al Qaeda used the cash-based *hawala* system that leaves no electronic record for money transfer (Posner 2003, 137). Money, moreover, as had been true of weapons, played no important role in the preparation of 9/11; the commission estimates that preparation and execution of the attack cost only $500,000. Money resources are a useful target only in a long-term effort to starve out an organization, but not effective in preventing a specific attack.

Another target of preventive policy was the safe haven Al Qaeda had found in Afghanistan. A safe haven is a typical need of “homeless” international terrorist organizations; national terrorist organizations need a supportive environment, too, but find this—if they do—in their own country. Bin Laden had returned to Afghanistan after Sudan, threatened with sanctions and pressed by Libya, finally denied him further sanctuary. To get at Al Qaeda’s safe haven there, diplomacy was needed. The U.S. had no direct lever on the Taliban; some general threats had been uttered against them after the attack on the USS Cole, but had no effect. The U.S. therefore urged Pakistan to get the Taliban to oust Bin Laden and deny Al Qaeda further sanctuary, but this, too, was unsuccessful.

To exert control, it is not sufficient to cut the supply chains of a terrorist organization. Equally important is the restriction of its action space. Communication, an important condition of terrorist action, is hardly subject to preventive control, thanks to the diffusion of electronic communication technology. Moreover, Al Qaeda often used couriers to communicate over wide distances. The commission in fact deals at length with terrorist travel, both crossing borders and moving about in a country, and complains about a “lax international security environment” (National Commission 2004, 366). International travel requires passports and visas; a visa is easier to get in some countries than in others, and there is less suspicion against a visa, say, from Germany than from Yemen. Moreover, countries like Malaysia did not require visas from Saudis. Such loopholes, systematically used by Al Qaeda, are a difficult target for preventive measures. Nor is it easy to prevent the manipulation of passports. The Al Qaeda office at Kandahar airport, where passports, visas and other documents could be altered (Ibid., 169), was beyond the reach of U.S. agencies. What remained was a defensive strategy. Attempts were made to tighten U.S. border controls, but before 9/11 such plans aborted. By the late 1990s, the Department of State had finally created a worldwide, real-time, electronic database of visa, law enforcement, and watchlist information, but this was put effectively into place only after 9/11.

**POLICY CONTEXT AND LIMITS TO THE CHOICE OF INSTRUMENTS**

The last section has shown that most of the important resources of Al Qaeda, and Al Qaeda itself, had remained intact by September 2001. It is instructive to spell out what, in addition to failures in threat perception, has impeded the choice of control measures that theoretically might have been effective.
One impediment to the choice of offensive measures is the fact that counterterrorism policy intersects with other policy fields. The general trade-off between security and civil liberties is a familiar example, but this did not really become an issue before 9/11 and the domestic security measures adopted following it. From the beginning, however, the transnational nature of Al Qaeda made fighting it an issue necessarily involving international relations, and hence touching on foreign policy. To induce Pakistan to prevail upon the Taliban to oust Bin Laden required changes in the standing U.S. policy of threatening Pakistan with sanctions in order to keep the Indo-Pakistani conflict from erupting into nuclear war. Foreign policy legacies also made the choice between threatening the Taliban and openly supporting the Northern Alliance a difficult one, and valuable time was lost as these options were weighed. Preventive measures can easily have negative side-effects on international relations. Thus the option of striking physically at Bin Laden was by-passed again and again for fear of the collateral damage (civilian casualties) that an air strike might cause, leading to a general deterioration of relations with Muslim countries. The fear of attacking the wrong target similarly impedes the choice of offensive measures. The—probably mistaken—air strike against a Sudanese factory believed to produce nerve gas for Bin Laden after the embassy bombings, and the erroneous bombing of the Chinese embassy in Belgrade, were one reason for Clinton not to order military retaliation to the attack on the USS Cole, which clearly bore the stamp of Al Qaeda but could not be linked directly and conclusively to Bin Laden.

Most importantly, the choice of potentially effective measures can be impeded because access to the target of control is restricted. Access is often particularly difficult if the target of control lies outside the national territory. Physical access was a problem for plans to capture Bin Laden and bring him before an American court, given that the U.S. had no undercover agents who could move freely and effectively about in Afghanistan. The so-called “tribal assets” that were to be used instead proved unreliable and ineffective. The U.S. also had no diplomatic access to the Taliban regime, since no formal relations existed, nor could the Taliban be threatened since they did not depend on the U.S. for anything important. Access, however, can also be limited domestically, for practical reasons as well as by the force of legal and constitutional norms. Legal arguments operated against killing Bin Laden. U.S. forces did not even seriously attempt to capture him alive before an indictment against him could be obtained, which it was hard to get for lack of legally convincing evidence. Constitutional norms impeded preventive measures that would affect the freedom of communication, of movement and of entering into private contracts—freedoms of vital importance for terrorist action. Borders, of course, can be controlled, and some potential participants in the 9/11 attacks were in fact denied visas. But those that did get to the U.S. were able to rent cars and apartments, to open accounts, to learn to fly, and to get airline passages. To live the life of a “sleeper” requires a loosely coupled social system with many control-free zones. Such an environment is found in the U.S., with its heterogeneous population, high valuation of individual freedom, and tolerance for people with strange habits and idiosyncratic beliefs. Moreover, in the U.S. “(a) large population lives outside the legal framework. Fraudulent documents could be easily obtained” (Ibid., 81).
attacks of 9/11 were in good part made possible by the opportunities the terrorists enjoyed to pursue their plan in the U.S. These opportunities, however, cannot be removed without making deep changes in the social and legal character of a country. This is likely the most serious barrier to the control of terrorist networks.

CONDITIONS FOR CONTROL OF A NETWORK ORGANIZATION

Effective control presupposes that the control structure, and the control strategy, “fit” the nature of the threat and the character of the “organization” generating it. Though the 9/11 Report does not discuss this, it is obvious that control meets with special difficulties if the target is a clandestinely operating network. A terrorist network that consists of semi-autonomous cells is more difficult to attack, and to defend against, than a hierarchical organization. A loosely coupled network is not disabled if individual cells are discovered and destroyed, and may even survive the elimination of its leader. It is also easier to know the structure of a hierarchical organization than the complex and fluid structure of a network. These problems do not only hold for Al Qaeda, but for terrorist networks generally, becoming the more compelling the more pronounced the network character of a terrorist organization is.

In order to control a clandestine network, it has been argued, the control structure should likewise adopt network features: “It takes networks to fight networks” (Arquilla and Ronfeldt 2001, 15; see also Slaughter 2004, 2). This reform recipe must, however, be understood correctly. The 9/11 Report shows that it was not too much hierarchy that was amiss in fighting Al Qaeda; on the contrary, the agencies that could have prevented Al Qaeda from reaching into the U.S. were too fragmented, pursued different goals, and made different assumptions about the nature and origin of terrorist threats. Nevertheless, the correct response to this would not have been to concentrate counter-terrorism in a single hierarchical organization. The 9/11 Commission never suggested such a thing; it diagnosed correctly that the crucial fault lay in the lack of cooperation and the sharing of information within and between agencies.

The 9/11 Report has shown that many a timely intervention was prevented by the lack of decentralized action capacity. But again it does not recommend empowering field offices to take speedy action independently. If the capacity to control the enemy by concerted action is not to be compromised, any movement from “hierarchy” to “network” must be balanced by integrating mechanisms. A shared sense of purpose, and the readiness to give each other unquestioned mutual support, could increase information sharing and cooperation in the national security community beyond what can be obtained by measures of formal organization. The importance of this attitudinal factor can be learned from Al Qaeda’s special mode of control: the actions of the semi-autonomous cells are not steered by commands or formal rules, but by the shared mission and a general strategy defined by the leadership. This control mode is predicated on a strong sense of unquestioning identification with the organization and its goal (Mayntz 2004).
In addition to the network character of Al Qaeda, its transnational expansion creates special challenges, because the national control structure is not congruent with the spatial structure of a transnational organization. The spatial incongruence between problem scope and control structure is a familiar issue in governance theory (Mayntz 2002, 23-25). As we know from the study of globalization and its effects on national policies, problems that originate outside of a country, but manifest themselves domestically, are particularly difficult to cope with. In terrorism control, the incongruence between the reach of a national control structure and the transnational nature of the control target affects not only the possibilities of intervention, but makes the collection of intelligence extremely difficult. Tardy intelligence in turn affects capability: Al Qaeda had not been targeted early enough for the U.S. to develop a network of “moles” and “assets.” Besides, the dominant orientation of public policy is toward domestic issues. Especially in a country as large as the U.S., the realization that developments taking place beyond its borders may pose a domestic threat takes time, and occurs often only when the point is drastically brought home by some dramatic event. The transnational nature of the control target also requires changes in wonted policy orientations. Law enforcement must extend its scope beyond normal criminals to potential terrorists, accepting foreign intelligence as equally relevant as domestic intelligence. Foreign policy based on diplomacy must become an intelligence-guided foreign policy.

The objective difficulty of collecting intelligence in foreign lands requires a strategic change from a doing-it-ourselves approach to a cooperative approach. Interventions directed at the geographically distributed site of a transnational terrorist network also raise access problems, which cannot be solved without international cooperation. Control over the acquisition of weapons and financial resources may not be much more difficult in the case of a transnational compared to a national terrorist organization, which also buys on the international black market. But the safe haven of a transnational terrorist network in a foreign country cannot be approached by domestic police forces; it requires a skillful use of diplomacy to motivate foreign governments to intervene instead. It is thus above all on the international plane that a network must be created for effective control. This does not only require cooperation among governments, but more importantly in intergovernmental networks at the agency level (Slaughter 2004). International cooperation among intelligence and law enforcement agencies is even more difficult to achieve than the cooperation of national agencies fulfilling different tasks. Threat perception is therefore crucial, because only a threat perceived as affecting all countries equally could motivate full cooperation. Again it is a shared sense of mission that could assure cooperation. This, then, lies at the core of the injunction to imitate the network character of the target for effective control: what is asked for is not horizontal differentiation, but a specific mode of integration.

**THE LESSONS FROM 9/11 IN CONCLUSION**

Without repeating in detail what has already been said about the requirements of controlling a terrorist network, we can briefly return in conclusion to the simple
control model with which we started. In the course of the analysis, this model has been
differentiated into four analytically distinct components: (1) information collection
and threat perception; (2) priority setting and allocation of attention; (3) mobilization
and choice of measures; and (4) action. These components are not to be understood as
separate phases in a stepwise causal process; they overlap in time and are linked by
feedback loops. Thus threat perception affects information collection as well as vice
versa, the results of action reflect back upon the choice of measures, and de facto
mobilization affects the allocation of attention. Still, the process is directed in so
far as phase 1 plays a special role in the model: threat perception triggers the process,
and the nature of the threat perceived shapes it as it proceeds. A specific threat for
instance activates a different set of control options than a highly general threat.

For each point in the model, it has been possible to identify—hypothetically, since
most of them were lacking—conditions of successful control. Some of these are
amenable to purposeful reform. Threat perception would gain from the existence
of an agency specially charged with the pooling and assessment of counterterrorism
intelligence it receives from both foreign and domestic sources. This agency could
develop information scanning and information pooling routines, involving all agen-
cies in the security community. The allocation of attention to the threat would gain
from the speedy, uninhibited distribution of threat information to all relevant actors,
in the security community as well as in the polity (e.g., congressional committees).
Mobilization should be a flexible response to particular threat situations, and use
a task-force strategy rather than, or in addition to, the institutionalization of fixed
routines. Mobilization needs a central authority able to command resources, to
enforce cooperation, and to see that needed capabilities are developed. Action,
finally, requires resources, and capabilities—legal, technical, and behavioral (e.g.,
language, covert action).

At each point in the model, it has also been possible to identify constraints that
cannot be manipulated relatively easily. Problems of access are a dominant con-
straint, except on priority setting, which instead suffers from an overload of policy
tasks. Some access problems have to do with the nature of the control object—a
clandestine, foreign-based network organization. Other constraints have to do with
the nature of the control subject—the government of a liberal, democratic, law-based
state. These constraints are ultimately based on the values defining the legitimacy of
a democratic regime; they can be overridden, but only at a cost that would ultimately
change the identity of the control subject. In addition to problems of access and legiti-
macy, there are constraints that follow from the interdependence of different policy
fields, and from objective difficulties of information processing, especially the recur-
sive relationship between information collection and threat perception. These vari-
ous constraints circumscribe the—relatively narrow—field where reforms could
improve the chances of control. The 9/11 Commission has rightly limited itself to
recommending the reform of conditions that can be manipulated with relative ease.
It is not the task of this paper to assess the reforms that the U.S. government has in
fact undertaken in the wake of the report. It is evident, however, that such an assess-
ment must take into account not only the control requirements, but also the obsta-
cles to meeting them identified in the preceding analysis.
REFERENCES


Renate Mayntz (mayntz@mpifg.de) is emeritus professor working at the Max Planck Institute for the Study of Societies, Cologne, Germany, of which she was the founding director. Her current research concentrates on issues of global governance.