9/11: Before and After

Michael Chertoff

WHERE WERE WE?

Until September 11, 2001, the United States had limited experience with terrorist attacks on our own soil, and only intermittent experience with attacks overseas. During the 1970s and 80s, airline hijackings and overseas bombings were the focus of most terrorist activity. In 1993, violent Islamist extremists bombed the World Trade Center, causing six deaths and more than a thousand injuries, but failing to significantly damage the structures themselves. During the next decade, several domestic focused Islamist terrorist plots were foiled at the planning stage; however, additional attacks were conducted overseas, by operatives of Hezbollah killing US service personnel in 1996 at the Khobar Towers complex in Saudi Arabia, by al Qaeda bombing of US embassies in East Africa in 1998, and the attack on the USS Cole near Yemen in 2000. The most deadly attack domestically during the 1990s was the Oklahoma City bombing, carried out by Timothy McVeigh, an anti-government extremist.

All of these attacks and attempts were addressed through the existing criminal justice system. Under that legal architecture, the Foreign Intelligence Surveillance Act and Title III of the Omnibus Crime Control and Safe Streets Act, as well as a host of other statutes and regulations, governed domestic intelligence collection. Exchange of information collected by foreign and domestic agencies was determined by a strict set of rules that was (perhaps somewhat incorrectly) interpreted as forbidding pure "intelligence" information from being collected for law enforcement purposes, and – conversely – made it difficult to share criminal justice-derived information with other agencies. When terrorists were apprehended either in the United States or abroad, they were accorded the treatment of any other criminal defendant, including receiving warnings about the right to silence, and a full-blown criminal jury trial.

The attacks of September 11, 2001 and the consequent retrospective investigations – such as the *9/11 Commission Report* – exposed the inadequacy of this architecture in addressing and thwarting further attacks. The inability to coordinate information collection and integration among various agencies led to the failure to identify patterns of behavior that might have provided warning of attack. Rules designed to govern electronic surveillance in the days of fixed land-line communications were difficult to apply to communications media such as mobile, disposable telephones or voice over internet communications. And even when terrorists were identified and apprehended, difficulties in providing evidence admissible in traditional courtroom proceedings left authorities with few avenues to detain or incapacitate them.

For the fundamental lesson was this: a counterterrorism architecture that is founded on criminal justice principles is fundamentally oriented to punishing those who have plotted or carried out attacks. But with the danger to innocent life posed by modern terrorism, prevention and not punishment becomes the critical driver for counterterrorism. And that required refashioning our legal tool set.

This refashioning focused on three elements of the counterterrorism process: intelligence collection, information integration, and terrorist incapacitation. The first refers to how we can better collect information in real time within the context of modern global communication, travel, and finance. The second focuses on how we can better combine and integrate that information once collected. And the third addresses how we can act on that information to incapacitate terrorists at the earliest stage before they can advance their operations.

WHERE ARE WE?

Intelligence Collection

In the wake of the attacks of September 11, the Bush Administration worked with Congress to update some of the rules governing interception of electronic communications and to streamline information requests. The USA PATRIOT Act, passed overwhelmingly, updated electronic surveillance rules to allow warrants to intercept individuals even when they frequently changed phones, and to grant access to Internet communications on the same basic terms as applicable to traditional telephone communications.

Somewhat more controversial was the implementation of regulations designed to collect routine traveler and financial information. During the past decade, the United States government implemented US VISIT, a program that captures fingerprints from all foreign travelers entering the United States. The government also exerted its right under the Chicago Aviation Convention to collect from the airlines commercial travel data relating to inbound travelers. This kind of data proved crucial in identifying high-risk travelers who are connected with known or suspected terrorists. Based on these "red flags," aviation and border security officials can now take a closer look at these travelers from among the millions who cross our borders each day.

The legality of these efforts has never been seriously challenged under US constitutional or statutory law. European data protection officials, however, resisted the use of commercial data on the grounds that it invaded the privacy of European travelers under European laws. The clash between international law giving the US the right to vet all incoming air travelers and European law seeking to cloak the privacy of those travelers threatened to cause disruption in the air industry. Fortunately this was averted for the time being through a US-European Union agreement that set an acceptable framework to accommodate security and privacy concerns.

A similar legal impasse arose from US government efforts to collect information from the so-called SWIFT system, an interbank network that exchanges global financial transactions every day. Government collection of this data under legal process allowed quick identification of suspicious movement of funds that might be used to support terrorist operations. This was precisely the type of smart intelligence collection advocated by the 9/11 Commission. In 2006, however, the *New York Times* chose to reveal the existence of the SWIFT collection program, thereby not only giving warning to terrorist financiers but provoking another privacy dispute with European authorities. Ironically, as even the *Times* acknowledged, the legal underpinnings of the SWIFT program were not open to serious question.

Perhaps the most controversial change in collection architecture arose from a dispute over the legality of an electronic surveillance program directed at intercepting certain international communications. The conflict was resolved by the passage of the FISA Act Amendments, which provided the US government with additional procedures and specific limitations to collecting information and intelligence from foreign terrorists and their affiliates located outside of the United States.

Information Integration

Perhaps the most well known finding of the 9/11 Commission was the missed warning signs that arose from a "failure to connect the dots" of individual intelligence items. This failure arose from institutional and cultural obstacles within the intelligence agencies, but also from a legal approach to the relationship between law enforcement and intelligence collection that built a substantial barrier to information sharing. The PATRIOT Act amended the law to dramatically lower the legal barrier to sharing, and to create a presumption of sharing rather than an inhibition against sharing. Ironically, a later court decision by the FISA Court of Review established that the previous interpretation of the FISA restriction on information sharing was unduly stringent, and reflected an overly cautious approach to the legal requirement.

Little legal controversy has arisen in the United States over information sharing,

although cultural barriers within the agencies remain, most recently demonstrated by the failure to integrate warning information of the would-be 2009 Christmas bomber, Umar Farouk Abdulmutallab. European views on information sharing remain dramatically different, however, with a strong bias against allowing integration of information from individual databases. For this reason, American and European officials have engaged in lengthy negotiations over the years about how willing the latter are to share biographic and biometric data even about individuals who are known criminals or terrorists. This information is not simply beneficial to the United States. Using known information about individuals, such as travel information, is an essential tool for detecting potentially dangerous individuals associated with terrorism and transnational criminal activity. Despite the differences between the US and European officials, information sharing agreements involving travel information and methods of payment exist today and incorporate appropriate privacy protections for individual personal information. As a result, the US has been able to enforce our border and immigration laws by disrupting, denying and dismantling terrorist travel as well as human trafficking and drug smuggling networks seeking to enter our nation.

Incapacitation

The most controversial elements of the new legal architecture for counterterrorism arise from the question of how to incapacitate someone apprehended here or overseas as a terrorist.

For the first several years after the September 11 attacks, Congress took no action to address the issue of incapacitation, as it had done with the issues of intelligence collection and sharing through the PATRIOT Act. The question of detention and punishment evolved within the Executive Branch. Alongside the customary criminal justice architecture, the Bush Administration established a military commission structure, drawing upon the historical model of military commissions that were impaneled during the Civil War and the Second World War and its aftermath. Military commissions – applicable only to non-US citizens – were designed to mete our punishment for the laws of war in the same way that the civilian justice system had punished terrorists for violating civilian laws.

Neither the courts nor the commissions, however, had a clear mechanism for detaining operatives who were terrorist threats before they were charged with a crime and punished. Such detention was available for those in the civilian system after charges were leveled, but that process required willingness to proceed to a trial in relatively short order. Especially for those caught on the battlefield overseas, where admissible evidence might be difficult to assemble, beginning the criminal justice process was impractical. Moreover, civilian arrest and charging triggered the right to silence, which frustrates the process of questioning for intelligence gathering, which was a primary objective when capturing terrorists.

Under these circumstances, the Bush Administration asserted the right to detain and hold enemy belligerents without trial or even military commission in line with the traditional authority of the military to hold prisoners in wartime. What was unclear in the initial stages of the conflict in Afghanistan was exactly what procedural mechanisms would be made available to assure those held were, in fact, affiliated with terrorists, and how this would mesh with various procedures mandated under the Geneva Convention.

Over the subsequent ten years, the evolution of the detention and incapacitation process has been ad hoc, if not at times chaotic. Contrary to conventional wisdom – indeed, conventional myth – the Bush Administration did not simply push all suspected terrorists into the military system. Generally, the Administration charged Americans and those captured on American soil in the civilian criminal justice system. Only two individuals apprehended in the United States were detained as military belligerents; each of these was eventually charged and convicted in US civilian courts. On the other hand, non-Americans apprehended overseas were generally detained in military facilities (including Guantanamo), and some began to be charged or processed through the military commission system. Thus, the Bush

Administration in practical terms deployed both civilian and military legal systems to handle issues of detention, with a rough presumption that those apprehended in the US and American citizens would be addressed through the former, and those non-citizens captured overseas would be addressed through the latter.

What was far less settled was the review to be afforded to those non-citizens held in military custody. Congress' failure to establish a process, and the Defense Department's restrictive approach to detainee rights, provoked ever more vigorous judicial review and eventually a significant overturning of parts of that system. While the Supreme Court affirmed the fundamental right of the president to detain and hold enemy belligerents during hostilities, the Court eventually granted at least detainees in Guantanamo some legal latitude to challenge the bases for their confinement by filing habeas corpus petitions in federal court. When Congress finally engaged in 2007 through the Military Commissions Act, the Congressional effort to limit this review was struck down by the Court. As a result, the exact scope of review for detainees in Guantanamo – let alone elsewhere – remains murky. A recent survey of individual cases suggests that the government prevails in the vast majority of challenges to date.

The advent of the Obama Administration was widely expected to herald a sea change in the approach to detention. After the president on his first day declared his intent to close Guantanamo, advocacy groups eagerly anticipated a return to the pre-9/11 legal architecture for detention, operating exclusively through the criminal justice system. Early returns suggested this change would occur, and the announced decision by Attorney General Eric Holder to try Khalid Sheikh Mohammed and other 9/11 coconspirators in federal court in New York was the apogee of this movement. But strong resistance – and perhaps a strong dose of reality triggered by the near success of the 2009 Christmas Day bomber – began to reverse direction. Over the last year, the Obama Administration has indicated that the 9/11 conspirators will be tried in military commissions, and while other terrorists have been tried in civilian courts, that mixed approach is largely consistent with the pragmatic approach of the Bush Administration. Perhaps most notable as a symbolic reversal, however, is the continued vitality of terrorist detention at Guantanamo, a practice that is likely to continue in the future given strong Congressional prohibitions against bringing Guantanamo terrorist detainees into the United States.

However inelegantly evolved, the current legal structure for incapacitating terrorists seems a rough compromise between security and civil liberties concerns, and is distinguished by a remarkable degree of continuity between the Bush and Obama Administrations. The executive branch's authority to detain enemy belligerents has been affirmed by both presidents, and by the Supreme Court. Some court review is afforded those held in the United States and in Guantanamo, but the rules of that review remain indistinct and uncertain. Military commissions are functioning under somewhat more generous rules for defendants, but no case has yet worked itself through the process. And legal adviser Harold Koh – who as dean of Yale Law School was an outspoken critic of the Bush Administration counterterrorism policy on civil liberties grounds – has recently issued a full throated defense of the president's right to order the killing of terrorists overseas.

WHERE SHOULD WE BE?

Although the legal architecture governing intelligence collection has adapted to new technologies in the last ten years, new challenges emerge. As cyber crime and "hacktivism" increase in frequency and consequence, the government's ability to monitor in real time for malicious code and similar cyber hacking tools is constrained by real uncertainty about the legal effects of the rules for electronic communications surveillance. If the malicious code is buried in the flow of Internet packets that delivers the stream of communication, does that mean those packets can only be scanned under the relatively stringent rules governing interception of communications? Or does the fact that the scanning is undertaken at the packet level mean surveillance rules should

not apply, since malicious computer instructions rather than intelligible communications are being sought? Sorting this legal conundrum, with far-reaching implications for both security and freedom of the Internet, is one of the overpowering legal challenges confronting us today.

By contrast, information sharing is on firmer legal footing in the United States. Here the continuing effort will be to resolve ongoing disputes with the European Union, which has reopened the controversy over American use of inbound airline passenger commercial data.

Finally, and most unsettled, are the legal rules that will govern detention of terrorist suspects. The current structure, fashioned case by case though the courts, leaves many questions unresolved. Issues of burdens of proof, what kind of evidence is admissible and what proof is sufficient, await definitive answers. Only Congress has the institutional capability and authority to fashion a comprehensive procedure for reviewing these cases that balance practical security concerns and fundamental fairness. Unless the administration and the legislators find the time and will to address these issues, uncertainties in our legal framework for detention will result in a system that is less than optimal from both security and liberty standpoints.

ABOUT THE AUTHOR

Michael Chertoff *was secretary of the US Department of Homeland Security from 2004 to 2009 and is presently co-founder and managing principal of The Chertoff Group and a senior of counsel at the law firm of Covington & Burling, LLP.*