International Law Studies - Volume 81
International Law Challenges:
Homeland Security and Combating Terrorism
Thomas McK. Sparks and Glenn M. Sulmasy (Editors)

I

The International Dimensions of Homeland Security

Ryan P. Stiles*

As I think we all know from the news and recent statements by both Attorney General Ashcroft and Secretary Ridge, we are entering an unprecedented period of threat as we go into the summer; a threat that is projected to continue through this November's elections. So what we're doing here has practical implications and will apply in the real world where terrorists routinely flout international law.

My goal for this morning is not to overlap with the discussions of the panels that will occupy much of the next three days of this conference. They will address many of the supporting issues regarding international implications of homeland security. My goal is to frame the debate: how, from a US Government perspective, the Bush Administration looks at homeland security and its objectives, and then to look at some specific ideas and concepts about how homeland security interacts with the international dimensions.

To frame the debate we must define homeland security. I think many people unfortunately skip that first definitional issue. The United States definition of homeland security is found in President Bush's July 2002 *National Strategy for Homeland Security*,[1] which was released as part of the Administration's proposal for creating a Department of Homeland Security. If you haven't read it, I encourage you to do so. The *Strategy* defines homeland security as "a concerted national

* Deputy Counsel, Homeland Security Council, the White House.

The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Dept. of the Navy, or Dept. of Defense.

effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism and minimize the damage and recovery from attacks that do occur."[2] Each piece of this definition is attached to a specific concept that requires additional analysis.

"Concerted national effort." Obviously the federal government has a critical role to play in homeland security. Yet the federal government alone cannot possibly protect the United States from future terrorist attacks. The Administration's approach to homeland security is based on the principles of shared responsibility and partnership with Congress, state and local governments, the private sector and the American people.

The concept of the first responder is one of the critical issues and one of the most difficult concepts in homeland security because the federal government is often not the first responder. In many cases, it will never be the first responder because anywhere from 80 to 90 percent of our critical infrastructure is in the hands of state and local governments, and the private sector.[3]

The federal government depends not only on partnerships with state and local governments but additionally with the private sector. It is a daunting task to coordinate all of those things, including such challenges as incompatible communication equipment. Federal government entities must be able to communicate with the first responders who inevitably have their own independent and different communications systems.

"Prevent." The first priority of homeland security is to prevent terrorist attacks. Post-9/11, the Federal Bureau of Investigation (FBI) (and the Department of Justice (DOJ) as well) transformed itself from being a traditional law enforcement agency to making its number one goal the prevention of terrorist attacks. That necessitates a shift in concept and a shift in tactics for the FBI; that shift is a good one.

It also makes the Department of Justice and the FBI's tasks significantly more difficult. Furthermore, it makes it increasingly difficult when we respond and deal with individual terrorists in the United States. In the past, most law enforcement consisted simply of investigation and response to terrorist attacks. If a terrorist attack occurred, the DOJ and FBI would investigate, identify the perpetrators, and put them on trial. This responsive mode did have limited success and did produce some convictions.

Now, however, the Department of Justice's success in accomplishing its new mission is challenged, if measured by a conviction rate, because now their intent is to prevent those attacks in the first place. By interrupting terrorist attacks before they occur, the DOJ will not have that clear chain of evidence that produced post-attack convictions. Now *intent* must be established before an attack occurs. That

means by necessity that the Department of Justice is probably going to lose a lot more cases in the short-term since they don't have the evidence trail they were able to produce during the post-attack trials because the plot has indeed been foiled.

That's not necessarily a bad thing, however. The Department of Justice is meticulous about which cases they bring to trial and which they don't. It is not a decision made by the individual US Attorney offices. Each terrorism case is scrutinized both in those offices and by the Criminal Division at Main Justice in Washington, D.C.

"Terrorist attacks." Homeland security is focused on terrorism in the United States. Terrorism is defined in the United States in a variety of ways but a definition that captures some of the core concepts of terrorism would be "any premeditated unlawful act, danger to human life or public welfare that is intended to intimidate or coerce civilian populations or governments."[4]

This definition captures the core concepts shared in the various iterations of the United States Code. As I'm sure many of the international practitioners here know, defining terrorism in the first instance is probably one of the most pressing problems facing the international community.

The United States has attempted to define the term at least for those who carry out attacks in this country. I think one of the key challenges for the international community is to develop an agreed upon definition of "terrorism." It is nearly impossible to eradicate something without having a definitional basis of what it is that's to be eradicated.

"Reducing America's Vulnerability." The United States is an ever-evolving, ever-changing target. As we shore up our defenses in one area, terrorists exploit vulnerabilities in other areas. A good example of that was a program called the Transits Without Visa Program that was shut down by the federal government in the summer of 2003 because of some specific intelligence that terrorists may be looking at that program as a way to enter the United States.[5]

An example of that program is an individual flying from South America to Europe who stops over in the United States for a connecting flight. Traditionally that person wasn't required to have a visa to "transit" the airport in the United States. However, that presented a seam for terrorists to exploit because they wouldn't have to go through the screening process with the Department of State or Department of Homeland Security. Thus, an individual could get on a plane in another country and, in some instances, land at an airport in the United States and simply walk unchallenged right out of the airport.

So you had a double vulnerability. One, terrorists would be on planes, which we know they like to use to attack the United States; and two, operationally they enter

the country in a fairly easy fashion. The United States has now closed that gap, although I do think a more secure program is probably in the offering at some point.

Once that program was ended, the terrorists looked for new vulnerabilities. So it is a constant challenge to make sure that when closing one gap or seam, new gaps and seams are not created. Avoiding new vulnerabilities is of great concern to those in the White House. Accordingly, when conducting our policy evaluations we work hard to ensure that the new, fresh policies do not inadvertently open a bigger seam when we close a smaller one.

"Minimizing the damage." As I mentioned at the outset, the greatest chance to respond effectively and minimize loss of life resides with our first responders, generally not with federal government entities. We're working with our state and local governments and the private sector to make sure they have their own homeland security plans to deal with whatever event may occur.

"Recovery." It is the intent of the United States Government to build and maintain various financial, legal and social systems that will ensure recovery from all forms of terrorism.

Responding to attacks on the homeland has been a vexing problem for the United States for the last 40 or 50 years. The old thinking about what type of attack would occur was focused primarily on nuclear strikes. Under that conceptualization, there would be the strike, the government would have to go somewhere, emerge at some later date and then repopulate the institutions.

Of course with the nuclear strike it was assumed that there would be an advance warning of an impending attack, so that continuity of government operation plans were premised on having some period of time to make preparations for the attack.

Now we have an entirely different model for attack and recovery: a "no-notice" event potentially aimed at decapitating the United States Government, to include the President and his staff, the cabinet departments, Congress and others. That model also means that we must look at other methods of making sure that our institutions survive because we're not going to be able to have 24 hours or even five or six hours to place those in key leadership positions in secure places.

Homeland security and national security are two obviously related concepts. But there is a core distinction. National security looks towards guaranteeing the sovereignty and independence of the United States with the values and institutions intact. This is slightly different from "homeland security." To provide the overarching strategy to ensure our national security, President Bush issued the *National Security Strategy of the United States*.[6] If read together with the *National*

Strategy for Homeland Security, you'll see they reflect an integrated concept, and that homeland security is a concept—not just a Department.

Within the concept of homeland security are the Continuity of Operation plans mentioned earlier; Critical Infrastructure and Protection, which is principally exercised within the United States, although some infrastructure is shared with Canada and Mexico, and defense against weapons of mass destruction (WMD). These obviously have to be dealt with if they enter the United States, but once they arrive on our shores we're already in trouble. Thus, much of the WMD efforts are focused overseas as we combat terrorism.

Another weapon of great concern is MANPADS (man-portable air defense systems). These short-range, ground-to-air missiles are one of the greatest threats to aviation around the world today. They're cheap, increasingly available on the black market, and exist in large numbers. Civil aircraft are virtual "sitting ducks" to terrorists who possess MANPADS. The United States is working to strengthen security over existing stockpiles and to prevent their continued proliferation. We are also working on measures to reduce the vulnerability of both military and civil aircraft to these weapons.

Prior to the establishment of the Department of Homeland Security (DHS) on November 25, 2002, funding for what we today call homeland security was spread throughout the government. But even in fiscal year 2003, the first year following the Department's establishment, only 51 percent of what the Office of Management and Budget considers homeland security spending was spent at DHS.[7] For fiscal year 2004, that figure is up to about 60 percent. In terms of actual total dollars, funding dramatically increased after September 11th, with about twice as many dollars devoted to homeland security in fiscal year 2003 as compared to the preceding year.

One organization of which you may be unaware is the Homeland Security Council (HSC). In October of 2001, the President created the Office of Homeland Security within the White House. Governor Tom Ridge became its head as a White House–appointed official.[8] Then when Congress created the Department of Homeland Security, Governor Ridge became "Secretary" Ridge and left the White House to become a cabinet secretary.

At the same time, the Office of Homeland Security transformed into the Homeland Security Council. The HSC's primary role is to serve as confidential adviser to the President on homeland security matters in much the same way as the National Security Council does on national security and foreign policy matters.

The Homeland Security Council's member's primary responsibility is to coordinate interagency efforts to ensure that the homeland is safe. HSC members work closely with the DHS staff, but also spend much of their time working with colleagues at the Department of State, Department of Justice, and the Central

Intelligence Agency. The reason, of course, is that the Department of Homeland Security can't do homeland security at the federal level by itself. It must coordinate its functions with those of other government agencies. Those functions are often based on funding priorities. I suspect I surprise no one when I say those agencies often don't agree on the best way forward. When that occurs a mediator is required and that's generally the role of the HSC.

The Homeland Security Council was built on the concept of the National Security Council,[9] which was created in 1947 by the National Security Act. The NSC and HSC are parallel organizations and sit side by side; one coordinating national security, the other homeland security. The NSC has no operational capacity, neither does the HSC. We simply try to resolve disputes and push efficient policy decision-making to secure the homeland.

America must pursue a sustained, steadfast, and systematic international agenda to counter the global terrorist threat and improve our homeland security. If the United States is 100 percent effective in homeland security, we will still have failed because most of the threats will be emerging overseas. If we aren't working cooperatively with our other States—our international partners—then we have really no chance at preventing terrorists from reaching our borders. If we can't screen cargo before it gets here, if we can't screen passengers before they step off the plane, ultimately we will lose the fight because those individuals will find methods to attack us even if we're secure within the borders. Thus the international agenda for homeland security is extremely important. We have to win our "away" games as well as our "home" games.

The following table lists the major homeland security initiatives with international dimensions.

Major Homeland Security Initiatives with International Dimensions

- Create "Smart Borders"
- Combat fraudulent travel documents
- Increase security of international law enforcement cooperation
- Intensify international law enforcement cooperation
- Help foreign nations fight terrorism
- Expand protection of transnational critical infrastructure
- Amplify international cooperation on homeland security S&T
- Amplify international cooperation in response to attacks
- Review international obligations to international treaties and laws

Many of these initiatives don't touch on the military components, which are more "overseas combating terrorism" than "homeland combating terrorism." I do this intentionally because I think our later panels will speak to those issues.

I also wanted to emphasize the international dimensions in a lot of projects that probably don't have a lot of visibility and are unknown to most people. The first is the creation of Smart Borders. We have a 5,500-mile border with Canada, a 1,900-mile border with Mexico, and 95,000 miles of shoreline. According to the 2000 census each and every year the United States admits 500 million people, including 330 million non-citizens through our borders.[10]

Our Smart Borders initiative must be able to deal with that flow of people, as well as the 11.2 million trucks and 2.2 million rail cars that cross the border annually. The Department of Homeland Security is spearheading the effort to create Smart Borders. America requires a border management system to keep pace with its expanding trade, while protecting the United States and its territories not only from terrorist attacks, but also illegal immigration, illegal drugs and other contraband.

The future of Smart Borders must integrate actions abroad to screen goods and people prior to their arrival in sovereign US territory. The border control agencies of the federal government also must have seamless information chain systems that permit communication among and between themselves and federal, state, and local law enforcement communities.

I want to address two specific programs within the Smart Borders initiative. One is the US-VISIT program that deals with land borders into the United States. The law requires that an automated entry/exit program be implemented at the 50 busiest land ports of entry by December 31, 2004 and all ports of entry by December 31, 2005.

The 50 busiest land ports of entry process 94 percent of the foreign visitors who enter and exit the United States through established border crossing. The concept of US-VISIT, which is being run by the Department of Homeland Security, is a continuum of security measures that begin before an individual enters the United States and continue through arrival and departure from the United States.

US-VISIT incorporates eligibility determinations made both by the Department of Homeland Security and, of course, the Department of State. Using biometrics such as finger scans and digital photographs, DHS will determine whether the person applying for entry to the United States is the same person who is issued the visa by the Department of State.

Additionally, the biometric and biographical data are checked against a watch list, thereby improving DHS's ability to make admissibility decisions, as well as the Department of State's ability to make visa determinations. US citizen entry

procedures are currently in place at 115 airports and 14 seaports. This year US-VISIT will be expanded to the 50 busiest land ports.

Since US-VISIT was launched in January 2004, it has already achieved some successes—mostly in the non-terrorist area to include drug smugglers, gangsters, and child molesters. Since the US Government stood up DHS, the Department of State has intercepted more than 200 people with prior suspected criminal or immigration violations. They include convicted rapists, drug traffickers, convicted armed robbers and numerous individuals committing visa fraud. The "non-terrorists" of today are creating pathways for the entry of bona fide terrorists of tomorrow.

Another important initiative to create smart, secure borders is addressed in section 343 of the Trade Act of 2002, as amended by section 108 of the Maritime Transportation Security Act, which requires that regulations be promulgated providing for the transmission to US Customs and Border Protection through an electronic data interchange system. The new system will provide information concerning cargo that is brought into or taken out of the United States prior to arrival or departure. This helps target specific cargos for potential, especially biological and chemical, weapons for inspection when they arrive at our borders. Of course, we can't have trucks backed up for miles on the Mexican border awaiting entry. If we wait until the cargo arrives at the point of entry to see what's on the manifest, we will have failed. We also will have failed our international partners because we will not have helped them facilitate their own internal economic stability.

A second major initiative is combating fraudulent travel documents. The Department of Justice, in conjunction with the Department of State, is spearheading this effort. They announced a new program that will contribute substantially to travel document security and our ability to impugn the movement of terrorists and other criminals. During the processing of travelers at ports of entry, if a hit occurs against the Interpol database, the hit will be verified with US authorities before action is taken against a bearer of such a passport. This is a significant step in the direction of curbing not only terrorism but also identity theft and other types of identity fraud. Travel document fraud, including the fraudulent application and use of the US passport, represents a serious and growing threat to our national security. However, it is not the individual who has stolen them who is necessarily the terrorist or expected terrorist. Often they are middlemen who steal passports and passport numbers, create fraudulent documents and sell them to the terrorists.

So we can't only concentrate on who we know or suspect of being international terrorists. We have to go at the middlemen who are facilitating the preparation of those fraudulent travel documents. Currently the Interpol database contains 1.6 million records reported by 41 different participating member countries. Of the 1.6 million records, approximately 60 percent are passports while 40 percent are

national identification documents. The United States has provided about 300,000 documents to that Interpol database. Although this is a relatively new initiative, it has had great success with the number of entries into the database increasing rapidly.

Contained within the initiative to combat fraudulent travel documents is the issue of biometric passports. The Administration has asked Congress to pass legislation to extend for two years the October 26, 2004 deadline by which countries must produce biometric passports to participate in the Visa Waiver Program. The problem is when Congress passed the law establishing the October 26, 2004 deadline it didn't have a complete understanding of what is required to produce an effective biometric passport. Biometric passports address a key weakness in our system for identifying terrorists. There are really two concepts. First, is the person standing before me the person that is identified in the travel documents? Second, is that person a good guy or bad guy?

If you fail at either one of those ends, you aren't going to catch known and suspected terrorists. A person may have perfectly good travel documents that aren't on any watch list. But if that person is someone other than the individual he purports to be, the validity of the travel documents is meaningless. That is the issue biometric passports are trying to address.

It is estimated that 13 million visitors from visa waiver countries enter the United States each year. Travelers from visa waiver countries are allowed to enter the United States for up to 90 days for business or pleasure using only a passport.

Our international partners tell us this is one of the key issues for them because it permits entry to citizens of those countries that the Department of State and Department of Homeland Security has determined as having secure documents. The Visa Waiver Program allows citizens of those countries easier entry into the United States. They don't have to go through the extended visa process. They can come in simply with their passport. We're working hard with our international partners to make sure this program continues in place while those countries come up with the technology and the decision-making necessary to continue to participate in the Visa Waiver Program.

The next issue I want to address is the increase in security of international shipping containers through a program called Container Security Initiative (CSI). Containerized shipping is a critical component of global trade because about 90 percent of the world's trade is transported in cargo containers.[11]

In the United States almost half of incoming trade by value arrives by containers on board ships. Nearly seven million cargo containers arrive on ships and are offloaded in U.S. seaports every year. In post–September 11th America, Container Security Initiative programs are key components to our homeland defense, based

on the idea that it makes sense to extend our zone of security outward so that American borders are the last line of defense and not the first.

Through CSI, maritime containers that pose a risk of compromise by terrorists are identified and examined at foreign ports before they are shipped to the United States. In so doing, the United States hopes to prevent terrorist attacks from being carried out by preventing the arrival of dangerous materials to the United States in the first instance.

CSI consists of four core elements: (1) using intelligence to identify and target containers that pose a risk; (2) prescreening those containers that pose a risk in the port of departure rather than the port of arrival in the United States; (3) using detection technology to screen containers that pose a risk; and, finally, (4) using smarter, tamper-resistant containers.

Obviously this would be an impossible initiative without our international partners. When we look to our international partners, despite what you may read on occasion, we have tremendous cooperation on all levels in all these initiatives I've discussed. They're brought into the decision-making process in the first instance and their considerations are taken into account. I think for the most part we've done a good job in working both through multilateral and bilateral negotiations to make sure their concerns are addressed.

Intensifying international law enforcement cooperation occurs on many levels. Perhaps the most important area is terrorist financing; the ability to freeze assets. The Patriot Act[12] greatly assists our international efforts to freeze assets, but obviously law enforcement cooperation occurs at intelligence and other levels as well.

I must again emphasize that the United States is committed to coordinating with our international partners to combat terrorism. As part of that coordination, the United States provides specialized training and assistance to help build the capability to combat terrorism. This occurs not only for military forces but also in the civilian agencies. Additionally, the United States hosts seminars to help our international partners draft their legislation, and to provide assistance regarding issues like MANPADS and bioweapons. The United States also provides equipment from time to time and science and technology advice on enhancing border security.

We're also expanding the protection of transnational critical infrastructure, especially with Canada and Mexico. As the events of August 2003, when failures in the power grid caused blackouts in large areas of northeastern United States and Ontario, Canada bore out, if you have an event in the United States that cascades to our neighbors, that is a big problem.

But it is a greater problem if it were to be part of a terrorist attack preventing first responders who rely on the power grid to respond and execute their initiatives. Because we share such a large border with our friends in Canada and Mexico, a lot of

our security, especially cybersecurity and obviously electrical security, crosses that border. So we work with them to help make sure that those systems are more secure from terrorist attack.

We also amplify international cooperation on homeland security through science and technology, a key concept being biosensors and also sensors of nuclear radioactive material. We work on science and technology with our international partners and once that technology is developed, we provide that to those friendly nations as well so that we can assist them in combating terrorism on their own shores as well as here. Other countries which haven't yet been targeted by terrorism still have an interest in ensuring that biological, chemical and nuclear weapons aren't being transited through their country.

We also work on improved cooperation and response to attacks. Last May, the United States staged a massive terrorist attack simulation to test our new plans. Canadian officials were involved in role playing. The scenario provided for simulated terrorist attacks in Seattle and Chicago. The hypothetical Chicago attack occurred at a Chicago Bulls–Toronto Raptors basketball game.

After the game the Raptors and their supporting contingent got back on their plane and returned to Canada, only then to realize that an attack had been carried out. So they had already spread the agent that was released in Chicago. This simulation allowed for cross-national planning on how the two countries could carry out a coordinated response, e.g., determining whether or not the border could be or should be shut down.

The United States, at the federal government level, looks to make sure we're positioned to deal with almost any imaginable scenario. We've gotten very good at doing "red cell" planning to hypothesize the full variety of attacks, although there is still considerable room for improvement. We'll never know until the next attack occurs, but the United States Government is very focused on making sure that there are preparations made for any kind of attack.

Finally, reviewing international obligations, international treaties and laws. We also work on a bilateral basis to negotiate and renegotiate Mutual Legal Assistance Treaties (MLATs). These assist US law enforcement agencies in gathering and exchanging information and evidence with foreign authorities for use in criminal trials.

We have many different international fora we can use to secure our international objectives. Obviously the United Nations plays an important role, as well as the Organization of American States and other regional groups, the G-8, and the International Civil Aviation Organization (ICAO).

One of the great concerns of the G-8 is the MANPADS threat. ICAO handles biometric passport issues. I am too technically illiterate to assist the determination

of whether there should be a 32-bit contactless chip embedded in a passport, but I do know we must have one uniform, worldwide readable document so we don't have some countries developing a technical form of passport.

In conclusion, as President Bush states, "We will not achieve these goals overnight. . . . [But] we will prevail against all who believe they can stand in the way of America's commitment to freedom, liberty, and our way of life."[13] But as we strive to reach those goals a key component is our international efforts. We will not secure America if we only secure the homeland from within our hard borders. We have to work with our international partners. We've had great success so far and we continue to hope to have that kind of success in the future.

Now many critics have said that the war on terror is not a winnable war, but the same critics said that about the Cold War as well. We must eradicate terror as an accepted tactic in warfare. Some people say again that's impossible, but I ask you to compare other forms of warfare and tactics that were previously acceptable and widespread, but now, for the most part, have been eradicated or substantially reduced as a tactic of war. Look at slavery, piracy, and genocide. Today these are among the universal crimes, but for hundreds, if not thousands, of years these were looked upon as acceptable methods of conducting war.

It's going to take a long time to drive terrorism into the same dustbin, but the US Government is giving its best to put an end to this evil. We again thank our international partners for their help in making us secure in our homeland and we will continue to work with them to secure theirs as well. Thank you.

Notes

1. Office of Homeland Security, National Strategy for Homeland Defense (July 2002), *available at* http://www.whitehouse.gov/homeland/book/.
2. *Id.* at 2.
3. Homeland Security Presidential Directive/Hspd-17, Critical Infrastructure Identification, Prioritization, and Protection ¶ 3 (Dec. 17, 2003), *available at* http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html.
4. National Strategy for Homeland Security, *supra* note 1, at 2.
5. The Transit Without Visa program was suspended on August 2, 2003. US Department of Homeland Security, Press Release, Aug. 2, 2003 ("Recent specific intelligence indicates that terrorist groups have been planning to exploit these transit programs to gain access to the U.S. or U.S. airspace without going through the consular screening process."), *available at* http://travel.state.gov/visa/visa_1248.html.
6. Various news organizations reported that the classified "Continuity of Operations" Plan was activated after 9/11. *See, e.g.*, Barton Gellman & Susan Schmidt, *Shadow Government Is at Work in Secret; After Attacks, Bush Ordered 100 Officials to Bunkers Away From Capital to Ensure Federal Survival,* WASHINGTON POST, Mar. 1, 2002, at A01.

7. Office of the President of the United States, The National Security Strategy of the United States (Sept. 2002), *reprinted in* 2002 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 947, *available at* http://www.whitehouse.gov/nsc/nss.pdf.
8. Office of Management and Budget, 2003 Report to Congress on Combating Terrorism 3 (Sept. 2003), *available at* http://www.whitehouse.gov/omb/inforeg/2003_combat_terr.pdf.
9. *Id.*
10. Homeland Security Presidential Directive-1, Organization and Operation of the Homeland Security Council (Oct. 29, 2001), *available at* http://www.whitehouse.gov/news/releases/ 2001/ 10/20011030-1.html.
11. For information on the Bush Administration's organization of the National Security Council, see National Security Presidential Directive-1, Organization of the National Security Council System (Feb 13, 2001), *available at* http://www.fas.org/irp/offdocs/nspd/nspd-1.htm.
12. National Strategy for Homeland Defense, *supra* note 1, at 21.
13. *Id.* at 12.
14. Pub. L. No. 107-56, 115 Stat. 272 (2001).
15. George W. Bush, The White House, July 16, 2002, *in* National Strategy for Homeland Defense, *supra* note 1.