Most of the contributions to this “Blue Book” focus on the possibility of computer network attacks by States as a methodology for so-called information warfare and the kinds of responses that may be taken consistently with the constraints of international law. In this chapter, however, the focus shifts from the use of force by States to criminal acts committed by private individuals not under the sponsorship or control of a State. With this shift of focus, the applicable legal regime becomes international criminal law rather than provisions of the UN Charter governing the use of force and the maintenance of international peace and security.

To be sure, “international criminal law” is an area of considerable definitional ambiguity. Some eminent commentators have denied its very existence. Other commentators, the majority, have defined international crimes as certain acts that constitute a crime against international law seeking only a tribunal with jurisdiction to apply that law and punish the criminal. Piracy is the prototypical example they cite. In response, the sceptics view piracy as solely a municipal law crime, the only question of international law being the extent of a State’s jurisdiction to apply its criminal law to an accused foreigner acting outside the territorial jurisdiction of the prescribing State.
Even for those crimes arguably constituting crimes under international as well as municipal law, it is necessary—in the absence of an international criminal court—to employ national law enforcement officials and national courts for purposes of apprehending, prosecuting, and punishing offenders. Accordingly, another dimension of "international criminal law" involves international cooperation in the enforcement of municipal criminal law. Although most efforts toward international cooperation in the enforcement of municipal criminal law have been on a bilateral or regional basis, the United Nations has played an increasingly important role in this area.

Considerable definitional ambiguity also surrounds the terms "terrorism" and "international terrorism." Despite strenuous efforts to do so, neither the United Nations nor its specialized agencies have been able to agree on a definition of "international terrorism." Rather, as we shall see later in this chapter, the United Nations has adopted a piecemeal approach to the problem through the adoption of separate conventions aimed at suppressing particular manifestations of terrorism. Although these treaty provisions are often loosely described as "antiterrorist," the acts that they cover are criminalized regardless of whether, in a particular case, they could be described as "terrorism."

Even at the domestic level, as illustrated by the US experience, defining international terrorism is a tricky proposition. Under US law there are a variety of definitions that serve a variety of purposes. Most important, at least at the federal level, there is no crime of "terrorism" per se. Rather, the Omnibus Diplomatic Security and Antiterrorism Act of 1986 provides US criminal jurisdiction over the killing of, or an act of physical violence with intent to cause serious bodily injury to or that results in such injury to, a US national outside the United States. Although the relevant chapter of the Act is entitled "Extra-territorial Jurisdiction over Terrorist Acts Abroad against United States Nationals," there is no requirement that the killing or violent act include the traditional elements of a terrorist act. Instead, the legislation incorporates the elements of terrorism as a limitation on prosecutorial discretion:

(e) LIMITATION ON PROSECUTION. No prosecution for any offense described in this Section shall be undertaken by the United States except on written certification of the Attorney General or the highest ranking subordinate of the Attorney General with responsibility for criminal prosecutions that, in the judgment of the certifying official, such offense was intended to coerce, intimidate, or retaliate against a government or a civilian population.
The conference report on the act makes it clear that the certification of the Attorney General or his designate is final and not subject to judicial review. The report also clarifies the meaning of the term “civilian population” by noting that it “includes a general population as well as other specific identifiable segments of society such as the membership of a religious faith or of a particular nationality . . . .” It is not necessary that either the targeted government or the civilian population be that of the United States.

As a general working definition for this chapter, I shall employ the definitions of terrorism utilized by the US Government for statistical and analytical purposes since 1983:

- The term “terrorism” means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.
- The term “international terrorism” means terrorism involving citizens or territory of more than one country.
- The term “terrorist group” means any group practicing, or that has significant subgroups that practice, international terrorism.

International terrorism is not a new phenomenon, and it is a topic that has been subjected to substantial scholarly (and some not so scholarly) analysis. Accordingly, in preparing this chapter, I have asked myself what I would call the Monty Python question: does the prospect of computer network attacks by terrorists constitute something “completely different,” or does it amount only to a new technique of attack for terrorists raising no new issues of law and policy? The answer, it appears, is that the possibility of computer network attacks does raise some new issues, although many of the old conundrums still pertain.

Efforts to combat international terrorism may take place at three different stages. The first, and ideal, stage is before a terrorist attack has occurred. Here the effort is to prevent a terrorist attack, either through the hardening of possible targets of terrorist attack or through intelligence work that allows law enforcement officials to learn of a planned attack in advance and intercept it.

The second stage involves responding to a terrorist attack while it is in progress, bringing it to an end, minimizing the damage it causes, and preventing panic among the general population. As we shall see, computer network attacks may present special challenges at this stage.

The third and last stage is where the perpetrators of the terrorist acts have succeeded in their mission, and it is necessary to apprehend them, submit them to prosecution before a tribunal with jurisdiction and fair procedures, and, if they are
Computer Network Attacks by Terrorists

found guilty, punish them. Here, too, computer network attacks may present special challenges.

In the sections that follow, I address some of the possible problems of combatting international terrorism at these three stages raised by the prospect of computer network attacks by terrorists. The final section sets forth some concluding observations.

Prevention

The Threat of Computer Network Attacks

Other chapters in this “Blue Book” discuss the nature of computer network attacks at great length and with substantial authority. No attempt is made to duplicate these efforts. Rather, this contribution attempts to discuss the concept of computer network attacks as a type of international criminal activity that might be engaged in by terrorists.

To this end it may be useful to distinguish, as Michael Schmitt has done in another context, between computer network attacks and information operations. As explained by Schmitt, “information operations” should be defined expansively to “encompass, among an array of other activities, virtually any nonconsensual actions intended to discover, alter, destroy, disrupt, or transfer data stored in a computer, manipulated by a computer, or transmitted through a computer network.” Moreover, information operations are subdivided into defensive and offensive information operations. Computer network attacks fall within the latter category and consist of “(o)perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.”

So defined, computer network attacks may take a variety of forms. They could be limited to the copying of sensitive data, which, depending on the circumstances, might constitute espionage, or include techniques for altering or destroying data and programs. Other computer network attacks might result in physical destruction, such as, most ominously, the “meltdown” of a nuclear reactor as a consequence of interference with its control system. Still other possible examples of computer network attacks have been suggested by Schmitt:

1. Trains are misrouted and crash after the computer systems controlling them are maliciously manipulated.

2. An information blockade is mounted to limit the flow of electronic information into or out of a target State.
3. Banking computer systems are broken into and their databases corrupted.

4. An automated municipal traffic control system is compromised, thereby causing massive traffic jams and frustrating responses by emergency fire, medical, and law enforcement vehicles.

5. Intrusion into the computer system controlling water distribution allows the intruder to rapidly open and close valves. This creates a hammer effect that eventually causes widespread pipe ruptures.

6. A logic bomb set to activate upon initiation of mass casualty operations is imbedded in a municipal emergency response computer system.16

As he recognizes, some of these examples are realistic while others may stretch credulity.

There is, moreover, the question of the technical capability of individual terrorists to engage in such computer network attacks without State support or sponsorship. In the past, the United States and other potential State targets of terrorist attack have benefitted from the relative technological incompetence of the terrorists.17 For many years now, however, computer systems have been recognized as being especially vulnerable to terrorist attack.18 And, in the words of one expert, “(t)he growing sophistication of high school students now entering college will ensure an ever greater pool of persons capable [of engaging in computer network attacks].”19

Another useful distinction to keep in mind is between those computer network attacks that (1) may cause disruption of vital systems leading to widespread inconvenience, possibly to some degree of public alarm, but that do not directly threaten life, and (2) those that directly threaten or appear directly to threaten human life.20 Most computer network attacks are more likely to fall within the first category than within the second.21

A major difficulty facing all efforts to prevent or combat computer network attacks is that they can be carried out remotely and often from great distances. Since anyone can access the Internet from anywhere in the world, law enforcement officials may have no idea where the attacker is located. Under such circumstances, law enforcement officials will not know the motive behind the attack or the identity of the attackers. Even if they succeed in tracking the source of the attack to an Internet Service Provider (ISP), this ISP may be a mere conduit, or the attack may actually have originated with a subscriber to that service.
Hardening of Targets

Identification and hardening of critical targets of possible terrorist attack has long been recognized as a crucial step in preventing terrorist attack. Virtually every major network—communications, electrical power, pipelines, and data—is vulnerable to terrorist attack. The vulnerability of many of these networks, however, depends on the would be attacker being able to identify the critical nodes. For example, taking out one refinery would have little effect on the oil industry. But attacks on certain pipelines could have devastating effects. Computer systems, on the other hand, are especially vulnerable, and "(i) it would not be difficult to seriously disrupt the Social Security System, nor would it be impossible to inflict vast harm to the Federal Reserve."23

This special vulnerability makes it especially difficult to harden computer networks against attack. Electronic vulnerabilities are often harder to guard than "traditional" vulnerabilities against terrorist attack. Part of the problem is the vastness and complexity of the information infrastructure. As of 1996, for example, the defense establishment reportedly had over 2.1 million computers, 10,000 local networks, and 100 long-distance networks.24 Moreover, although it is clear that this infrastructure is subjected to a large number of attacks, the number of reported incidents is probably just the tip of the iceberg because, according to estimates, only about one in 150 attacks is actually detected and reported.25 The same pattern is likely present in other sectors of the US Government and in the vast private sector.

Security technologies and products—such as, for example, firewalls26 and smart cards27—may afford some protection, but they are hardly foolproof.28 Additionally, as new security tools are developed, computer network attackers learn how to defeat them or exploit other vulnerabilities.

Human failings greatly compound the problem, as when inexperienced or untrained users accidentally publicize their passwords or weak passwords are chosen which can be easily guessed. Accordingly, it is generally agreed that training in information security for personnel, including top management, is a crucial element for a good information systems security program.29

Intelligence Operations

There is general agreement that the collection and use of intelligence is an effective tool in combating terrorism. Ideally, the gathering of intelligence serves a preventive role and enables law enforcement officials to intercept terrorists at an early stage, before they inflict injury on persons or property. However, even
with respect to terrorists who employ more conventional methods than computers, this has proven to be a difficult task to accomplish.

Problems may arise at the national level. In the United States, for example, there is evidence that constraints imposed on intelligence activities from 1975 to 1980 may have adversely affected the timing and availability of preventive intelligence to the extent that the proportion of cases in which violence or other crimes were prevented declined.30

The Fourth Amendment to the US Constitution prohibits unreasonable searches and seizures and clearly would apply to law enforcement searches of computer data bases in the United States.

The risk to privacy concerns would be especially great under such circumstances. The Foreign Intelligence Surveillance Act of 197831 regulates electronic surveillance of foreign powers and the agents of foreign powers and defines “foreign power” to include “a group engaged in international terrorism or activities in preparation therefor.”32 The act sets up a special court consisting of seven district judges who hear and determine applications for electronic surveillance warrants. The statute allows warrantless electronic acquisition of communications exclusively between foreign powers not involving a substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.33

The United States Supreme Court has held that the Fourth Amendment does not apply to searches and seizures abroad of property owned by non-US citizens or permanent residents.34 However, search and seizure of material located in computers abroad may be viewed by foreign sovereigns as a violation of their territorial sovereignty. Moreover, the standard techniques for obtaining criminal evidence abroad—letters rogatory and mutual legal assistance treaties, for example—are designed to assist in apprehending, prosecuting, and punishing those who have already committed crimes, not as a device to gather intelligence regarding the possible future commission of a crime.

Under these circumstances, then, cooperation between US and foreign intelligence officers would seem vital. Nonetheless, foreign laws protecting privacy are, if anything, more stringent than those of the United States. Therefore, in either the domestic or the international context, the challenge to balance privacy and individual rights concerns with the requirements of law enforcement is formidable.35

Management of an On-going Terrorist Incident

The goals of counter-terrorism efforts during an ongoing terrorist incident would at a minimum be threefold: (1) to bring the terrorist attack to an end;
Computer Network Attacks by Terrorists

(2) to minimize the damage caused by the attack; and (3) to prevent panic and restore order. A computer network attack by terrorists would probably complicate and make fulfillment of these goals more difficult.

This would especially be the case if the computer attack was widespread and well coordinated and involved both governmental and private sector targets. Suppose, for example, that simultaneous computer attacks disrupted the US command and control infrastructure so that individual military units were unable to communicate with each other or with a central command; air traffic control systems were also disrupted, causing planes to crash with substantial loss of life; a “computer worm” or “virus” traveled from computer to computer across a network, damaging data and causing systems to crash. Assume further that the sources of these attacks could not be easily located. The challenges facing authorities seeking to bring the attacks quickly to a halt and to prevent panic would be monumental.

Panic might be particularly pronounced because many otherwise informed people tend to dismiss the prospect of computer network attacks as a minor risk. According to Richard Clarke, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council:

[CEOs of big corporations] think I’m talking about a 14-year-old hacking into their Web sites. I’m talking about people shutting down a city’s electricity, shutting down 911 systems, shutting down telephone networks and transportation systems. You black out a city, people die. Black out lots of cities, lots of people die. It’s as bad as being attacked by bombs. . . . Imagine a few years from now a President goes forth and orders troops to move. The lights go out, the phones don’t ring, the trains don’t move. That’s what we mean by an electronic Pearl Harbor.36

Apprehension, Prosecution, and Punishment

Apprehension

Before a suspect can be apprehended, he or she must be located. As has often been noted elsewhere in this “Blue Book,” computer network attackers can frustrate investigatory efforts by “looping and weaving” their attacks through several foreign countries, thus greatly complicating the efforts of investigators to follow their trail. If the suspect is located, it then becomes necessary to induce law enforcement officials of the place where he is located to take him into custody. They will not do so unless the computer network attack in question would
be a crime under their local law. This requirement would also have to be met as a condition of extradition because of the “double criminality” requirement in virtually all extradition treaties.

Prosecution and Punishment

If the suspect is apprehended abroad, the issue arises whether, and if so where, he will be prosecuted. At present, no multilateral antiterrorism convention expressly covers computer attacks. However, depending on the circumstances, it is possible that one of the existing conventions—e.g., the Convention for Suppression of Unlawful Acts Against the Safety of Civil Aviation or even the not yet in force International Convention for the Suppression of Terrorist Bombing—could apply. If so, the extradite or prosecute approach that is the keystone of these conventions would govern the rights and obligations of the States parties.

Under this approach a State party that apprehends an alleged offender in its territory must either extradite him or submit his case to its own authorities for purposes of prosecution. Strictly speaking, none of the antiterrorism conventions alone creates an obligation to extradite; by requiring the submission of alleged offenders for prosecution if extradition fails, they contain an inducement to extradite. Moreover, a legal basis for extradition is provided either in the convention or through incorporation of the offenses mentioned in the convention into existing or future extradition treaties between the parties. To varying degrees, the conventions also obligate the parties to take the important practical step of attempting to apprehend the accused and hold him in custody.

The most important goal of these provisions is to ensure prosecution of the accused. To this end, the conventions state quite strongly the alternative obligation either to extradite or to submit the accused for prosecution. The obligation, however, is not to try the accused, much less to punish him, but to submit the case to be considered for prosecution by the appropriate national prosecuting authority. If the prosecuting State’s criminal justice system lacks integrity, the risk of political intervention in the prosecution or at trial exists. Such intervention may prevent the trial or conviction of the accused, or act as a mitigating influence at the sentencing stage.

Even if the prosecuting State’s criminal justice system functions with integrity, it may be very difficult to obtain the evidence necessary to convict the accused when the alleged offense was committed in another country. This very practical impediment to conviction can be removed only by patient and sustained efforts to develop and expand “judicial assistance” and other forms of
cooperation between the law enforcement and judicial systems of different countries. The conventions create an obligation to cooperate in this regard, but, as will be demonstrated in greater detail later, this obligation is often difficult for countries with different types of legal systems to meet, even assuming that they act in complete good faith. The difficulty may be even greater when cybercrime is involved.

Many, perhaps most, instances of computer network attack would not be covered by the antiterrorist conventions. In such cases, the United States would need to engage in a process of rendition to get the suspect before a US court. Besides extradition, the forms of rendition include exclusion, deportation, and abduction. Subject perhaps to very limited exceptions, abduction is illegal, and exclusion and deportation involve unilateral action by the State of refuge and are relatively informal measures subject to a relative lack of legal limitations. Extradition is generally recognized as the only process of rendition that satisfactorily protects the rights of an accused. Assuming that the United States did not wish or could not convince the State of refuge to deport the accused, it would try to extradite her. The obstacles to the success of this endeavor, however, could be considerable.

**Barriers to Extradition**

First, the requested country would be under no obligation to extradite absent an extradition treaty between it and the United States. Although the United States is a party to more than 100 bilateral extradition treaties and to the Inter-American Convention on Extradition with 13 parties, the absence of an extradition treaty has been a problem in some high profile cases. Moreover, although the United States would be entitled to use most of the antiterrorist conventions for purposes of extradition, it has chosen not to do so. The United States also will not itself extradite a person to a requesting country in the absence of an extradition treaty.

Even with an extradition treaty, the extradition process is often fraught with difficulties. As already noted, many, if not most, US extradition treaties require that the action in question be a crime in both the requesting and requested country for extradition to take place. This dual criminality requirement can pose major problems in computer crime cases. Although the United States has amended its criminal code to penalize a wide range of computer crimes, other countries have been slow in doing the same. This has resulted in cases where the United States has identified the location of a perpetrator of a computer crime, but has been unable to secure her extradition because the act in question was not a crime under the law of the country where the perpetrator was
found and the extradition treaty between the United States and the country in question contained a dual criminality requirement.\textsuperscript{52} Although there is widespread recognition that countries need to reach a consensus as to which computer related activities should be criminalized, this is a process that will take some time.\textsuperscript{53}

Under the extradition law of a number of countries, it is necessary for a requesting country to present the requested country with satisfactory (to the requested country) evidence that a crime covered by the treaty has been committed.\textsuperscript{54} This has especially been the case with common law countries. Great Britain, for example, traditionally required prima facie evidence of a crime covered by the extradition treaty. For countries on the continent of Europe, which had no such requirement, this posed a “mystery” as to precisely how much evidence was required to meet this standard.\textsuperscript{55} In 1982, approximately a third of the applications made to the United Kingdom under its extradition treaties failed and the most common cause of failure was the requesting State’s inability to satisfy the prima facie requirement.\textsuperscript{56} Because of this record of failure in the extradition process, Great Britain amended its extradition law in 1989 to exclude selectively the prima facie requirement in relation to certain States, and then ratified the European Extradition Convention, which has no such requirement.\textsuperscript{57} Instead, the convention requires only that the request be accompanied by a certificate of conviction or the warrant for arrest, a statement of the offense and a copy of the necessary laws.\textsuperscript{58} The US test of “probable cause,” which requires only that there be reasonable grounds to make it proper that an accused be tried for the crime, has not proven to be a barrier to extradition.\textsuperscript{59}

The prima facie requirement has been defended on the ground that it operates as a necessary protection for the individual who otherwise may be removed to another State merely because he is suspected of having committed a crime covered by the extradition treaty.\textsuperscript{60} Be that as it may, there is no doubt that the prima facie requirement makes extradition more difficult. This difficulty may be especially great if computer network attacks are involved because the barriers to gathering evidence in such cases, as already noted, may be substantial.

Another barrier to the extradition of international terrorists may be the refusal of some countries, especially those with a civil law background, to extradite their nationals.\textsuperscript{61} One of the grounds advanced by Libya in refusing to surrender two Libyan members of the Libyan secret service who were indicted by a grand jury of the District of Columbia in November 1991 for the December 1987 explosion of Pan Am flight 103 over Lockerbie, Scotland that killed 270 persons, including 189 Americans, was that the Libyan Constitution prohibited the extradition of Libyan nationals.\textsuperscript{62}
The Austrian Supreme Court has gone so far to claim that the provision in the Austrian Constitution prohibiting the extradition of nationals reflected “a generally recognized rule of international law.” Even the government of the United Kingdom reserves the right not to extradite nationals where there is no extradition treaty with the requesting State and the latter is seeking the fugitive’s return under a multilateral, antiterrorist convention.

At least in Europe, however, the situation changed substantially in 1996, when the European Union concluded a Convention Relating to Extradition of Nationals. The first paragraph of Article 7 of that convention provides that extradition may not be refused on the ground that the “person claimed is a national of the requested Member State.” But the second and third paragraphs of Article 7 of the convention permit a five year rolling reservation allowing member States to refuse extradition of their nationals. According to Geoff Gilbert, the Explanatory Report “makes clear several matters:”

First, that the Nordic members of the European Union will no longer classify domiciled aliens as nationals for the purposes of intra-EU extradition; secondly, that the protection of nationals might be achieved by those States which do not ordinarily extradite nationals, by entering a reservation that any sentence imposed by the requesting State will be served in the requested State; next, that given that some States are constitutionally prohibited from extraditing their own nationals, that they review the scope of the restriction at least once every five years; and, finally, that reservations are not indefinite and can lapse.

In other words, even with the conclusion of the 1996 convention civil law countries resist extraditing their own nationals.

On the other hand, as to certain international crimes, there is some evidence that civil law States are beginning to relax their previous practice of never extraditing their nationals, at least in their extradition relations with common law States. For example, the 1983 extradition treaty between the United States and Italy specifically provides that extradition shall not be refused on grounds of nationality and is aimed at combatting the coordinated organized crime in the two countries. Further, the increasing practice of repatriating prisoners to serve their sentences in their own country has reportedly convinced some civil law countries in Europe to extradite their nationals to common law countries.

Outside of Europe there has also been some movement, albeit it slow and tentative. In 1979 the United States and Colombia concluded an extradition treaty that allowed for the surrender of nationals. The treaty was a response to the inability of the United States to secure the extradition of Colombian
nationals who had imported illegal drugs, especially cocaine, into the United States and who had so corrupted Colombian law enforcement officials that trial in Colombia was not possible. The new extradition treaty was extremely unpopular in Colombia, however, and in 1988 the Colombia Supreme Court declared the treaty unconstitutional. Repeated efforts by the United States resulted in Colombia passing a new law allowing for the extradition of its nationals in 1997, and at this writing Colombia has extradited two drug suspects to the United States.

Relations between the United States and Mexico concerning the possible extradition of Mexican nationals have been especially tortuous. Under the US-Mexican Extradition Treaty, neither party is required to extradite its nationals. Rather, Article 9 of the treaty gives both parties the option to prosecute as an alternative to extradition, and from 1978 until 1996 Mexico, as a matter of policy, refused to extradite its citizens to the United States. Moreover, allegedly as a result of corruption among Mexican law enforcement officials, persons that the United States sought to extradite, especially for drug trafficking, were often not prosecuted in Mexico. Finally, in 1996, Mexico surrendered four of its citizens to the United States for prosecution, two of them for drug trafficking. Nonetheless, since that time, Mexico’s record, from the US perspective, has been unsatisfactory, and there have been recent court challenges to the extradition of Mexican nationals that may have to be resolved by Mexico’s highest court.

Recognition by the requested country that the requesting country has jurisdiction to try the accused is a prerequisite to extradition. The complexity of civil and criminal jurisdictional issues in cyberspace, however, is just beginning to be recognized.

In recent years, at both the state and the federal level, the United States has extended the death penalty to more and more crimes, including terrorist crimes. By contrast, since World War II, opposition to the death penalty has resulted in many countries including clauses in extradition treaties that exclude extradition where the requesting State retains the death penalty and is unwilling or unable to provide assurances that this penalty will not be carried out if the accused is extradited. This development has greatly complicated US extradition relations with other countries, including cases involving terrorist crimes.

Another important development in recent years has been the increasing importance of human rights considerations as a limitation on extradition. Opposition to the death penalty in the Western European States is based in large part on the belief that it violates fundamental human rights values. On the other hand, as noted by John Dugard and Christine Van den Wyngaert, “[t]oday states are irreconcilably divided over the morality and effectiveness of the death
penalty," and as a result its imposition is not prohibited by general international law. Under certain circumstances, however, according to some authorities, imposition of the death penalty may constitute cruel, inhuman, or degrading treatment or punishment, and thus violate general international law norms.

The best known of these authorities is the decision of the European Court of Human Rights in Soering v. United Kingdom. Soering, a West German national, murdered his girlfriend’s parents in Virginia and fled to the United Kingdom. In response to a US request, the United Kingdom ordered his extradition to the United States. Soering, however, petitioned the European Commission of Human Rights, which referred his case to the European Court of Human Rights. The court held that the United Kingdom had an obligation under Article 3 of the European Convention of Human Rights, which prohibits torture and inhuman or degrading treatment or punishment, not to extradite Soering to the United States where there was a real risk that he would be subjected to inhuman or degrading treatment by being kept on death row for a prolonged period in the state of Virginia. Eventually Soering was extradited to the United States when the United Kingdom received assurances from US officials that he would not be subjected to the death penalty.

Although it is not a judicial body with authority to hand down a decision binding on parties to a dispute, the Human Rights Committee, which is the body established by the International Covenant on Civil and Political Rights to supervise implementation of the covenant by States parties, found in Ng v. Canada that California’s practice of executing by gas asphyxiation, which might take over ten minutes to cause death, resulted in prolonged suffering constituting cruel and inhuman treatment within the meaning of Article 7 of the covenant. On the basis of this finding, the committee was of the opinion that Canada, which could reasonably have foreseen that Ng would be executed in this way, had violated its obligations under the covenant by extraditing him to the United States.

In 1980 Alona Evans identified the political offense exception, which is grounded, at least in part, in human rights considerations, as the “hot issue” of extradition law. At that time, the political exception was regarded as perhaps the primary barrier to the extradition of international terrorists. But in recent years States have taken a variety of steps to limit or even to eliminate the political offense exception as a defense to extradition, and it is unclear whether the political offense exception remains a major barrier to extradition at the present time.

As an alternative to or a substitute for the political offense exception, extradition treaties may permit the accused to claim that he will not receive a fair trial in the requesting country. Article 3(a) of the United States–United Kingdom
John F. Murphy

Supplementary Extradition Treaty of 1985, for example, expressly permits a judicial inquiry into whether the extraditee will be “prejudiced at his trial or punished, detained or restricted in his personal liberty by reason of his race, religion, nationality or political opinions.” This so-called “humanitarian exception” was inserted because of the concern of some US Senators that the elimination of the political offense exception effected by the supplementary extradition treaty would result in inadequate protection for extraditees. By giving the courts the responsibility of ruling on allegations of an unfair trial, the treaty waters down the rule of noninquiry US courts normally apply, under which the courts defer to the executive branch to make the decision as to the validity of such allegations. In practice, however, courts in the United States have been extremely reluctant to make a finding that would reflect on the standards of justice in the United Kingdom. On the other hand, courts in both the United States and Canada have held that the rule of noninquiry is not absolute and that it will not be followed if the likely treatment in the requesting State would be shocking or simply unacceptable.

As a result of these many barriers, the extradition process has been described as “a creaking steam engine of an affair.” Former US Attorney General Benjamin R. Civiletti was of the view that extradition laws belong to “the world of the horse and buggy and the steamship, not in the world of commercial jet air transportation and high speed telecommunications.” It is therefore not surprising that law enforcement officials have often turned to alternative forms of rendition in their efforts to bring alleged offenders to a forum for prosecution.

Alternatives to Extradition

One alternative to extradition that has been employed with some frequency in Europe is “hot pursuit.” This approach allows the police authorities of one State to cross the borders of a neighboring State in hot pursuit of a fleeing fugitive, and it is consistent with the policy of internal open borders that the European Union has followed since 1993. Also, the Schengen Accord of 1990 concluded among Belgium, the Federal Republic of Germany, France, Luxembourg, and the Netherlands, allows the police agencies of the States parties to cross borders in hot pursuit, although the precise scope of this authority is a matter of dispute. Outside of Europe, the doctrine of hot pursuit is apparently not widely utilized as a method of rendition.

The methods of rendition most often utilized as alternatives to extradition are exclusion and deportation. Exclusion may occur when fugitives are apprehended as they attempt to enter a country, and deportation may be an option
when fugitives are arrested within a country’s territory. In US practice, not surprisingly, many of these exclusions and deportations have involved Canada and Mexico and have been directed towards persons accused of drug trafficking.¹⁰⁵ Both exclusion and deportation are civil processes, designed for immigration control and dominated by the executive. As a consequence, exclusion and deportation proceedings utilized for rendition purposes do not apply criminal justice standards, either with respect to the interests of the States involved or to protection of the accused. Unlike extradition, exclusion and deportation rarely involve a formal request by a State seeking a return of the alleged offender. On the contrary, exclusion and deportation are effected at the instance of a territorial State.¹⁰⁶

Perhaps the most controversial use of deportation as an alternative to extradition was the case of Joseph Doherty. After unsuccessful attempts to extradite Doherty, a member of the Provisional Irish Republican Army, from the United States to the United Kingdom, where he was wanted for his role in the death of a British soldier and for his escape from prison, because of decisions by US courts that his offenses fell within the political offense exception in the US-UK extradition treaty,¹⁰⁷ the United States Supreme Court upheld his deportation to Northern Ireland after long and complicated legal proceedings.¹⁰⁸ Apparently, the deportation of Doherty was handled as a purely internal matter and not in response to a request from the United Kingdom that he be deported. Although some commentators have argued that it is improper for one State to request another to deport an individual as a means of circumventing extradition procedures, US courts have repeatedly held that the existence of an extradition treaty between the United States and another country does not bar the use of other means to obtain custody over a criminal located abroad.¹⁰⁹ In contrast, complicity between the French government and another government to use deportation as an alternative to extradition may reportedly be the basis for dismissal of the prosecution.¹¹⁰

The most controversial alternative to extradition has, of course, been abduction or kidnaping of alleged offenders. Both commentators and State practice support the general proposition that international law prohibits a State from sending its agents into another State to abduct an individual residing there without that other State’s permission.¹¹¹ Abductions would seem prima facie to violate a principal rule of international law, which states that a nation is absolutely sovereign within the boundaries of its own territory.

There is at least an argument, however, that abduction may be consistent with international law under certain extraordinary circumstances. Despite the prohibition against the use of unilateral force in Article 2(4) of the UN Charter, Article 51 allows a victim of an armed attack to use force to defend itself pending
action by the Security Council.\textsuperscript{112} Justification of a government sponsored abduction of a fugitive necessarily requires characterizing the actions of the fugitive as an "armed attack" within the meaning of Article 51.\textsuperscript{113} This characterization has most often been applied to cases of terrorism and drug trafficking. In 1989, expressly repudiating an earlier opinion to the contrary in 1980,\textsuperscript{114} then Assistant Attorney General William Barr produced a legal opinion that international law allowed US law enforcement officials to make extraterritorial arrests under certain circumstances.\textsuperscript{115} Testifying before Congress, Barr stated on behalf of the Department of Justice:

[T]here are instances where extraterritorial arrest without the host sovereign's consent may be justified under international law. For example, in response to an actual or threatened terrorist attack, we would have good grounds under general principles of international law to justify extraterritorial law enforcement actions over a foreign sovereign's objections. Moreover, in appropriate circumstances we may have a sound basis under international law to take action against large-scale drug traffickers being given safe haven by a government acting in complicity with their criminal enterprise. Thus, it may well be that the President will choose to direct extraterritorial arrests only when he believes that he is justified in doing so as a matter of self-defense under international law.\textsuperscript{116}

The validity of Mr. Barr's proposition has been subject to sharp debate.\textsuperscript{117} In practice, however, at least as of this writing, the US Government has made no extraterritorial arrests of alleged terrorists without the consent of the territorial sovereign. The 1987 sting operation that resulted in the apprehension of Fawas Younis took place on a US ship in the Mediterranean after Younis had been lured there by US agents.\textsuperscript{118}

In contrast, the US Government has made extraterritorial arrests in drug trafficking cases.\textsuperscript{119} The most controversial of these was the 1990 apprehension and deportation to the United States of Dr. Humberto Alvarez-Machain by Mexican agents paid by the US Drug Enforcement Agency (DEA). Dr. Alvarez-Machain was a prominent Mexican gynecologist who had been indicted for the kidnap and murder of Enrique Camarena, a DEA agent stationed in Guadalajara. After strong protests by the Mexican Government, and a circuit court opinion holding that the abduction violated the US-Mexico extradition treaty,\textsuperscript{120} the US Supreme Court ruled that the abduction was not barred by the extradition treaty and that US courts could exercise jurisdiction over the case.\textsuperscript{121} Although the majority opinion all but conceded by way of dicta that the abduction violated norms of customary international law,\textsuperscript{122} the court did not address the issue
of whether this might constitute a basis for US courts to decline jurisdiction. Courts in several other countries have ruled that they have discretion in such circumstances to refuse to exercise jurisdiction.\textsuperscript{123}

The Supreme Court's decision in \textit{Alvarez-Machain} has been subjected to sharp criticism.\textsuperscript{124} Be that as it may, Geoff Gilbert has suggested that, paradoxically, the Court's decision may "hasten the demise of State sponsored kidnaps of alleged international criminals, for it has brought to the fore this attempt to authorize the 'manifestly illegal.'"\textsuperscript{125} Indeed, in the wake of \textit{Alvarez-Machain}, the Bush Administration quickly responded with assurances that it had no intention of either increasing or institutionalizing the practice of extraterritorial abductions.\textsuperscript{126} Also, in 1994, the United States and Mexico concluded a Treaty to Prohibit Transborder Abductions\textsuperscript{127} (which, however, as of this writing has not yet been sent to the Senate for its advice and consent to ratification).

\textbf{Mutual Assistance in Criminal Matters}

Regardless of what method of rendition is used, once an accused is before a US court, it is necessary to prove his guilt beyond a reasonable doubt. But if the evidence to do this is located abroad, and cannot be obtained, the successful rendition of the accused may be a pyrrhic victory.

Moreover, the legal mechanisms for obtaining evidence abroad for use in criminal proceedings are less than satisfactory.\textsuperscript{128} Letters rogatory, the standard mechanism, are especially ill-suited for obtaining evidence regarding computer crimes. Letters rogatory require an application to a foreign court and usually provide for advance notice and participation by opposing parties. Hence, the procedure is relatively public, as compared to the US practice of conducting criminal investigations under the veil of grand jury secrecy. It is, moreover, even under the best of circumstances extremely slow, and foreign tribunals may give limited or no assistance at the pre-indictment phase of a case. In any event, the decision of foreign tribunals to respond favorably is purely discretionary, since the letters rogatory practice is based on comity considerations rather than on binding international legal norms.

Because they create binding international legal obligations for the States parties, Mutual Legal Assistance Treaties (MLATs) may be of greater value. As of November 15, 1997, the United States had 23 MLATs in force.\textsuperscript{129} They provide prosecutors with a channel for sending requests for assistance in obtaining evidence through a Central Authority in one country\textsuperscript{130} to a corresponding prosecutorial authority in the other country, which oversees the prompt execution of the request. Under MLATs, foreign prosecutorial authorities will normally seek
mandatory process under their law, when necessary, to execute the request and keep it confidential to the extent possible.

The US MLATs contain a provision that obligates a requested country to conduct searches and seizures on behalf of a requesting country if the request includes information justifying such action under the laws of the requested country. Only a few of these MLATs, however, apply broadly to all law enforcement investigations and prosecutions, rather than only to certain types of offenses such as drug trafficking and money laundering. Additionally, the political offense exception is often available in MLATs and can be a barrier to obtaining the necessary evidence. Finally, even though the MLAT process is usually much faster than letters rogatory, as we have seen, evidence of computer crime can be rapidly transferred out of the jurisdiction of the requested country to other countries with whom the United States has no MLAT.

Especially for the collection of electronic evidence, MLATs, while an improvement on letters rogatory, are unequal to the task. The problem has been aptly posed by Michael Sussmann: “How does law enforcement collect electronic evidence that may be scattered across several different countries, can be deleted or altered with one click of a mouse, may be encrypted, and will ultimately need to be authenticated in another country’s court?” The ability to delete or alter electronic evidence with the click of a mouse renders even the relatively rapid procedures available under MLATs hopelessly slow and cumbersome. Accordingly, in Sussmann’s view:

[W]hen electronic evidence is sought, there may be a need for mechanisms such as a “preservation of evidence request” or “protected seizure,” which would work as follows. Where there is a particularized concern about the loss of electronic evidence, a country would make an informal international request that the data immediately be preserved. This could be accomplished in a number of ways, from having a telecommunications carrier or ISP [Internet Service Provider] copy and store a customer’s data, to actually seizing a criminal’s computer and securing, but not searching, it for a short period of time. Once data is (sic) protected from loss, expedited processes would provide the foreign country with formal documentation to authorize the issuance of a domestic search warrant or similar process.

As Sussmann notes, the US Code provides for a form of “preservation of evidence” request. Most other countries apparently do not have such provisions in their laws, although the need for them has recently been recognized, at least in principle. Once such provisions are in place, it may be necessary to revise the
MLATs to ensure that the law enforcement officials of the other party to the treaty will be able to take advantage of them.

Transborder searches and seizures are an especially difficult problem when electronic evidence is involved. Although paper documents are normally located in the same country as the person being investigated, this is not necessarily the case with electronic evidence. To the contrary, electronic data may be stored in another country or countries to keep them beyond the reach of law enforcement.

Transborder searches consist of a law enforcement officer in his or her own country accessing a computer in another country to obtain electronic evidence. Such searches may take place unknowingly. For example, if an investigator searches the computer of a domestic corporation, the data accessed through that search may be located in another country unbeknownst to the investigator. Unconsented to transborder searches of electronic evidence may be viewed by the country where the search occurs as a violation of its sovereignty or even of its criminal law, subjecting the individual investigator to possible criminal liability. From a law enforcement perspective, it is necessary for countries to agree on principles permitting transborder searches under clearly defined but broad circumstances. Others may be of the view that the need to protect data in a particular country outweighs law enforcement concerns. Although this issue is currently being debated in several international forums, its outcome is far from certain.

If an investigator succeeds in accessing electronic evidence, wherever it may be located, the evidence may be unintelligible because it is encrypted, i.e., scrambled to protect its confidentiality. The need for encryption is widely recognized as necessary to protect the confidentiality of e-mail traffic, stored data, and commercial transactions. However, when criminals use encryption for communications or data storage, they may severely hamper criminal investigations by preventing timely access to the content of seized or intercepted data. Hence, law enforcement officials are concerned that they be able to obtain the “keys” to decrypt encrypted data. In contrast, privacy advocates, cyber-rights groups, and defense counsel, among others, oppose granting law enforcement broad authority in this area.

Moreover, according to Phillip Reitinger, the principal legal obstacle to law enforcement access to “plaintext” (i.e., unencrypted or decrypted text) and keys is the Fifth Amendment privilege against self-incrimination. Reitinger concludes that a grand jury subpoena can order the production of the plaintext of encrypted documents and the production of documents that reveal keys. He further concludes, however, that whether law enforcement
can compel production of keys that are only known, rather than recorded, is an open question.139

At this writing, Congress has passed, and the President has signed, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001."140 This highly controversial legislation, which critics have argued could be used overzealously and harm innocent people,141 provides, for the first time, for federal monitoring of computer communications, allowing investigators to track the sending and receiving of e-mail and Internet connections. They will not, however, be able to read the content of such computer communications without first obtaining a warrant. The legislation will also, among other things, allow investigators to conduct unannounced searches of property owned or occupied by terrorism suspects and to share information from federal criminal investigations with intelligence agencies for the first time.

There is also controversy over the efforts of law enforcement officials to secure laws that would permit them to sidestep encryption.142 Regardless of how this debate is resolved, there is a need to reach agreement at the international level on decryption support services. As Michael Sussmann has pointed out, only the more modern of US MLATs contain provisions that are flexible enough to accommodate such newer forms of assistance as decryption services.143 Even these MLATs do not specifically address the subject of decryption, and there currently are no international commitments to provide decryption support. Although there are discussions and negotiations underway in various international forums designed to resolve the problems of access to computers by law enforcement persons and encryption along with related issues, the final outcome of these efforts is uncertain at this writing.144

**Some Concluding Observations**

From the foregoing discussion, one may safely conclude that the prospect of computer network attacks by terrorists has only recently begun to receive the attention—from statesmen, law enforcement officials, and scholars—that it deserves. Moreover, although international terrorism has long been a subject of intense scrutiny, the prospect of computer network attacks by terrorists introduces legal and operational complications for those engaged in efforts to prevent, contain, and punish terrorist attacks.

Law and the legal process has traditionally lagged technological developments and the computer revolution is no exception. In particular, the speed with which computers operate and the anonymity of their operators create
challenges for the "snail pace" of traditional law enforcement methods. Also, as we have seen, at the domestic level in the United States there is currently a significant tension between the perceived needs of law enforcement and protection of the privacy rights of US citizens. At the international level this tension is likely to be as intense, perhaps even more, than it is in the United States, since the Europeans, for example, strongly emphasize the protection of privacy in their law and practice.\textsuperscript{145}

Although there are strenuous efforts in various international fora to resolve these problems, including the adoption of a draft convention on computer crime under the auspices of the Council of Europe, the success of these endeavors is by no means assured. Nonetheless, it has long been a truism that international cooperation is crucial to successful efforts to combat international terrorism.\textsuperscript{146} This truism applies \textit{a fortiori} to efforts to combat computer network attacks by terrorists.

Moreover, international cooperation in combating terrorism has often taken the form of informal arrangements and liaisons between law enforcement officials in several countries, rather than the use of formal arrangements spelled out in treaties or national legislation. In view of the speed with which law enforcement personnel need to act to cope with a computer network attack, informality is likely to be required to give law enforcement the flexibility it needs to operate successfully. At the same time, the need for appropriate restraints on law enforcement of the kind provided by legal regulation is also great in the field of computer crime. The struggle to find the right balance is likely to continue for some time to come.

Notes

\textsuperscript{a} The author would like to thank Brian T. Gorman, a graduate of Villanova University School of Law, for research assistance on this paper and Gregory Schaffer of the Division of Computer Crimes and Intellectual Property in the US Department of Justice for providing him with a copy of an article by his colleague, Michael Susmann, prior to publication.


6. 18 US Code §2331(c).
8. Id.
9. The reasons the Omnibus Diplomatic Security and Antiterrorism Act of 1986 dropped any reference to terrorism as an element of the offense itself are enlightening. These reasons have been well summarized by Geoffrey Levitt, formally an attorney in the Office of the Legal Adviser, Department of State, who worked on the act. Levitt first suggests that the political intent element characteristic of a "generic" definition of terrorism is inherently vague, and then states:

In the US legal context, this flaw poses fundamental constitutional problems. The due process clause requires that criminal statutes "give a person of ordinary intelligence fair warning that his contemplated conduct is forbidden by the statute." When first amendment concerns are also involved, as they would of necessity be in any statute that included a politically oriented intent element, this requirement has even greater force. Even were such problems somehow resolved, the breadth of a generic intent element would severely complicate the task of prosecutors, who would be required to prove beyond a reasonable doubt the presence of a particular political motivation. Consequently, this would leave the Government open to accusations of selective prosecution based on the political views of defendants. A separate but substantial problem would be the likely absence of a similar intent element in the penal law of extradition treaty partners, thus removing the factor of dual criminality, a prerequisite to extradition—and one must wonder what the point would be of an international terrorism offense for which the United States could not successfully request the extradition of a suspected offender. . . .


10. Under the US Government approach, the term "noncombatant" is "interpreted to include, in addition to civilians, military personnel who at the time of the incident are unarmed or not on duty. . . . We also consider as acts of terrorism attacks on military installations or on armed military personnel when a state of military hostilities does not exist at the site, such as bombings against US bases in Europe, the Philippines, or elsewhere." US Department of State, Patterns of Global Terrorism: 1998, April 1999, at vi, note 2.

11. Id. at vi–vii.
12. Monty Python fans will remember that their television show began with the proclamation "and now for something completely different."
14. Id. at 890.
15. Id. at 888.
16. Id. at 892–93.
17. See, e.g., the summary of the remarks of J. Christian Kessler in JOHN F. MURPHY, LEGAL ASPECTS OF INTERNATIONAL TERRORISM; SUMMARY REPORT OF AN INTERNATIONAL CONFERENCE 45 (1980).
18. Summary of Remarks of Robert Kupperman in id. at 41–42.
20. See MURPHY, supra note 17, at 35.
22. Summary of Remarks of Robert Kupperman, supra note 18, at 42.
Computer Network Attacks by Terrorists

23. Id.


25. Id.

26. “Firewalls are hardware and software components that protect one set of system resources (e.g., host systems, local area networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic.” Id. at 4, note 2.

27. “Smart cards are access cards containing encoded information and sometimes a microprocessor and a user interface. The encoded information and/or the information generated by the processor are used to gain access to a computer system or facility.” Id. at 4, note 3.

28. On the contrary, according to a recent article, “there is no such thing as a secure computer network.” Charles C. Mann, The Mole in the Machine, THE NEW YORK TIMES MAGAZINE, July 25, 1999, at 32. In this article, Mann quotes Eugene H. Spafford, Director of the Purdue Center for Education and Research in Information Assurance and Security, as stating: “The only system that is truly secure is one that is switched off and unplugged, locked in a titanium safe, buried in a concrete vault on the bottom of the sea and surrounded by very highly paid armed guards.” Id.

29. See Abstracts of GAO Reports and Testimony, supra note 24, at 19, 23–24.


32. Id., § 1801(a)(4).

33. Id., § 1802(a)(1) (A)(1) and (B).


35. To be sure, there are success stories. For example, according to the Washington Post, after the embassy bombings in Nairobi and Dar es Salaam, the United States revealed that, in 1997, it had successfully prevented two terrorist attacks on US embassies by infiltrating terrorist cells and intercepting electronic communications. See Walter Pincus & Vernon Loeb, CIA Blocked Two Attacks Last Year, Washington Post, Aug. 11, 1998, at A16.


38. For discussion, see GEOFF GILBERT, TRANSNATIONAL FUGITIVE OFFENDERS IN INTERNATIONAL LAW 104–16 (1998).

39. On June 29, 2001, however, a Draft Convention on Cyber-Crime was adopted under the auspices of the Council of Europe, and on September 19, 2001, was approved by the Council of Europe’s Ministers’ Deputies. The Convention will be open for signature by nonmember states that participated in the four year drafting exercise, including the United States, which has observer status at the Council of Europe. The convention is controversial, and it remains to be seen how many states become parties. See Council of Europe, Draft Convention on Cyber-Crime and Explanatory Memorandum Related Thereto, Draft Explanatory Report (June 29, 1001), http://www.conventions.coe.int/treaty/en/projects/finalcyberrapex.htm.

346
42. See, e.g., id., art. 8.
43. See, e.g., id., art. 7.
45. See id. at 179.
49. See MURPHY, supra note 46, at 43.
51. See Sussmann, supra note 37, at 464-65.
52. Id. at 463-64.
53. Id. at 464-65.
54. See GILBERT, supra note 38, at 119-27.
55. Id. at 119.
56. Id. at 120.
57. Id. at 120-21.
58. Id. at 121.
59. Id. at 123.
60. Id. at 126.
61. Id. at 175-84.
62. See Joyner & Rothbaum, supra note 48, at 250-51.
63. As quoted in GILBERT, supra note 38, at 176.
64. Id. at 177.
66. Id. at 179.
68. GILBERT, supra note 38, at 180.
70. See GILBERT, supra note 38, at 179-80.
71. Id. at 180, note 19.
73. For discussion, see Argiro Kosmetatos, U.S.-Mexican Extradition Policy: Were the Predictions Right about Alvarez?, 22 FORDHAM INTERNATIONAL LAW JOURNAL 1064 (1999); Bruce Zagaris & Julia Padierna Peralta, Mexico-United States Extradition and Alternatives: From Fugitive

347
Slaves to Drug Traffickers—150 Years and Beyond the Rio Grande’s Winding Courses, 12 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 519 (1997).

75. See Kosmetatos, supra note 73, at 1066.
76. Id.
77. Id.
79. For an excellent discussion of these issues, see PERRITT, supra note 37.
81. See GILBERT, supra note 38, at 155-69.
82. In the Venezia case, an Italian court suggested that the assurances by the United States that the death penalty would not be imposed was an insufficient guarantee, since such assurances by the executive could not bind the judiciary. Venezia v. Ministero di Grazia e Giustizia, Corte cost., June 27, 1996, n. 223, 79 Rivista Di Diritto Internazionale 815 (1996). For discussion, see Andrea Bianchi, case note, 91 AMERICAN JOURNAL OF INTERNATIONAL LAW 727 (1997).
84. Id. at 197.
86. See FRANK NEWMAN & DAVID WEISSBRODT, INTERNATIONAL HUMAN RIGHTS 477 (2d ed. 1996).
87. 999 U.N.T.S. 171, 6 INTERNATIONAL LEGAL MATERIALS 368 (1967).
88. 98 INTERNATIONAL LAW REPORTS 479 (1993).
89. As Christine Van den Wyngaert has pointed out, the political offense exception has a humanitarian basis in that it is viewed as protection against an unfair trial in the requesting State which, as the target of the political crime, might be inclined to function as both judge and jury. CHRISTINE VAN DEN WYNGAERT, THE POLITICAL OFFENSE EXCEPTION TO EXTRADITION 2 (1980). At the same time, she criticizes this rationale on the ground that it is not always true that political offenders are likely to be subject to an unfair and partial trial. Id. at 4.
91. For further discussion, see MURPHY, supra note 46, at 45-70.
93. According to the ILA Report, “today the political offence exception is not accepted in a wide range of circumstances.” Id. at 224.
95. See Dugard & Van den Wyngaert, supra note 83, at 190.
96. Id., noting In re Requested Extradition of Smyth, 61 F. 3d 711,722 (9th Cir. 1995); In re Extradition of Howard, 996 F. 2d 1320,1331-33 (1st Cir. 1993).
97. Id., noting several US and Canadian decisions.
98. See GILBERT, supra note 38, at 1, quoting THE OBSERVOR, April 29, 1979, at 4.
99. Quoted in id. at 1.
100. Id. at 363.
102. GILBERT, supra note 38, at 363.
103. There is no discussion of cases outside of Europe in GILBERT, and the doctrine of hot pursuit is not even mentioned by Nadelmann in Ethan Nadelmann, *The Evolution of United States Evolution in the International Rendition of Fugitive Criminals*, 25 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 813 (1993), perhaps the most extensive recent examination of methods of rendition.
104. GILBERT, supra note 38, at 376.
105. Nadelmann, supra note 103, at 860.
106. See generally, GILBERT, supra note 38, at 364–77.
111. In the words of the Restatement (Third) of the Foreign Relations Law of the United States: “A state’s law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.” *RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES*, § 432(2).
112. UN CHARTER art. 2(4):
All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

UN CHARTER art. 51:
Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

113. The International Court of Justice, in *Nicaragua v. United States*, 1986 I.C.J. Rep. 14, para. 195, stated, “[i]n the case of individual self-defense, the exercise of this right is subject to the State concerned having been the victim of an armed attack.”


is no suggestion in any of the background of Article 51 or the massive writing on that article that it can be used to justify law enforcement directed against individual suspects located in another state.

118. For a brief discussion of the Younis case, see Nadelmann, supra note 103, at 866.

119. Id. at 870–74.

120. United States v. Alvarez-Machain, 946 F. 2d 1466 (9th Cir. 1991).


122. Id. at 669. ("Respondent and his Amici may be correct that respondent's abduction was "shocking" ... and that it may be in violation of general international law principles ... Mexico has protested the abduction of respondent through diplomatic notes ... and the decision of whether respondent should be returned to Mexico, as a matter outside of the Treaty, is a matter for the Executive Branch.")

123. See Murphy & Dumont, supra note 44, at 206–08; GILBERT, supra note 38, at 352–60.


125. GILBERT, supra note 38, at 352.


128. For general discussion of MLATs, see ETHAN A. NADELMANN, COPS ACROSS BORDERS 312–96 (1993).


130. The Criminal Division's Office of International Affairs of the Department of Justice serves as the Central Authority for all US MLATs.

131. Sussmann, supra note 37, at 472.

132. Id. at 473.


134. Id. at 474.

135. Id. at 475.

136. Id.

137. Id. at 475–76.


139. Id. at 173. See also David Goldstone & Betty-Ellen Shave, International Dimensions of Crimes in Cyberspace, 22 FORDHAM INTERNATIONAL LAW JOURNAL 1924 (1999).


143. Sussmann, supra note 37, at 476, note 78. As an example, Sussmann notes that Article 1, paragraph 2(h) of the US-UK MLAT provides for "such other assistance as may be agreed between Central Authorities."
144. Id. at 478–90.


146. For an exploration of this theme, see John F. Murphy, *The Need for International Cooperation in Combating Terrorism*, 15 *Terrorism* 381 (1990).