I. INTRODUCTION

Terrorism is one of the most heinous crimes against humanity and human rights. It takes thousands of lives for no reason other than political publicity. There is not a single religion in the world that condones this behavior and yet its impact seems to grow with every passing year. Human rights crimes are seen as crimes against mankind and there are some that see terrorism in the same way, a common law offense against mankind. When one thinks of a terrorist, typically a Middle Eastern Arab
man comes to mind, as seen when the authorities were trying to find suspects for both the New York City World Trade Center and Oklahoma City bombings. However, American society was shocked to learn that anyone could be a terrorist. The Oklahoma City bombing was masterminded not by a Middle Eastern Arab but a white American citizen. Besides being identified as an Arab, many terrorists have been viewed as "madmen or fanatics" with whom one cannot negotiate.\(^1\) Thus, in order to rationalize their behavior they are described as psychotic or even psychosociological.\(^2\) But, if we cannot even profile a terrorist how are we expected to combat terrorism?

The remainder of this paper will attempt to answer that question by detailing how the world is addressing the problem of terrorism and working as a global entity to eliminate it. Being that terrorism has evolved over time, this paper will focus on pre-computer advancements and post-computer advancements in a comparative fashion. Part I will lay out the issues that will be addressed in the remainder of the paper. Part II will focus on terrorism and the evolution it has made over time. Included in this part, is a section dealing with definitional information so that everyone is aware of the problem and understands how it is being addressed and categorized. The next section profiles terrorism from the 1970's and contrasts it with more modern terrorism. After that is a description of statistics outlining the results of various terrorist attacks over the years along with agency profiles. Next, is a section providing quotes from various world leaders and nations in general pledging their commitment to the eradication of terrorism. Following this is a national response to terrorism, focusing mainly on laws and conventions from around the world that have been enacted as a way to deal with the international problem of terrorism. And finally, the last section in Part II will focus on new threats to the world community in the face of terrorism.

Part III of this paper will focus on cyberterrorism, the newest form of terrorism to have evolved. The first section in this part provides the reader with a brief explanation of cyberterrorism along with numerous definitions that have been used when describing cybercrime and cyberterrorism in general. The following section is one of the reasons for the growth of cyberterrorism. A section on the impact of cyberterrorism and the coverage that it is able to maintain as a result of the advancements in technology is next. After this section there will be some descriptions of

---

1. **TERRORISM AND INTERNATIONAL LAW** 5 (Rosalyn Higgins and Maurice Flory eds. 1997). This viewpoint is contrasted in a subsequent footnote that indicates that yesterday's terrorists were ones' that the authorities could in fact negotiate with.

2. *Id.*
the new weapons used in cyberterrorism and the threat that they cause. Lastly, there is a section detailing what is being done to deal with cyberterrorism followed by critics who do not see cyberterrorism as an issue that should be addressed at all right now. And finally, Part IV of this paper will include conclusions reached.

II. TERRORISM

A. Definitional Explanations

Terrorism is a form of political behavior and has been defined as "the threat or use of violence in order to create extreme fear and anxiety in a target group so as to coerce them to meet political objectives of the perpetrators." It differs from revolutionary action in that it does not seek to overthrow the government but rather strives for short-term intimidation. Normally, the terrorist act demonstrates the fragility of a certain social or political order by attacking the State, its symbols or representatives of power. Thus, a terrorist act seems to be an "act of violence committed by an individual with a political, ideological, social, or even religious aim." According to the Immigration and Naturalization Service (INS), a terrorist organization is defined as "one whose leadership, or whose members, with the knowledge, approval, or acquiescence of the leadership, have taken part in terrorist activities." There are three requirements that the Secretary of State can use to identify a terrorist organization. They are: 1) if the organization is a foreign organization, 2) if the organization engages in terrorist activities, and 3) if the organization threatens the security of United States nationals or the national security of the United States. As of December 2000, there were twenty nine such terrorist organizations listed. A terrorist organization designation can be

3. Id. at 4.
5. Higgins, supra note 1, at 4.
6. Id. at 150 (acknowledging that through their actions many terrorists are able to address the nation and lay down conditions or espouse their beliefs).
7. Id.
9. Id. (defining "national security" as the "national defense, foreign relations, or economic interests of the United States").
10. Id. (listing the organizations in alphabetical order as follows: Abu Nidal Organization, Abu Sayyaf Group, al Qa’ida, Armed Islamic Group, Aum Shinrikyo, Basque Fatherland and Liberty, Gama’a al-Islamiyya, Hamas, Harakat ul-Mujahideen, Hezbollah, Islamic Movement of
set aside, however by the United States Court of Appeals for the District of Columbia. However, the court cannot set aside a designation based on the Secretary of State’s determination that the organization threatens the security of United States nationals or the national security of the United States.

B. Contrasting Decades of Terrorism

In the 1970’s and 1980’s terrorism consisted of the taking of hostages, plane hijacking and destruction, and attacks by bombs, mostly car bombs. The terrorists themselves were small bands of nationals with identifiable goals and usually had to do with the denial of the right of self-determination or resistance to physical and oppressive foreign occupation. Even if the organization took on a religious name the terrorism itself was seen as secular in nature. Old terrorist leaders were ones you could negotiate with, accept a cease-fire, exchange for hostages or the return of the remains of dead soldiers in exchange for terrorist prisoners. This old terror provided a contract like environment between the state and the terrorist organization. In many instances, these terrorists were seen as

Uzbekistan*, Japanese Red Army*, al-Jihad, Kach*, Kahane Chai, Kurdistan Worker’s Party, Liberation Tigers of Tamil Eelam, Mujahedin-e Khalq Organization, National Liberation Army, Palestine Islamic Jihad-Shaqqai Faction, Palestine Liberation Front B Abu Abbas Faction, Popular Front for the Liberation of Palestine, Popular Front for the Liberation of Palestine B General Command, Revolutionary Armed Forces of Colombia, Revolutionary Organization 17 November, Revolutionary People’s Liberation Party / Front, Revolutionary People’s Struggle*, Shining Path, and Tupac Amaru Revolutionary* Movement.) * As of October 5, 2001, the organizations indicated with an * were dropped from the list, while the Revolutionary Nuclei was added to the list. State Dept. Redesignates 25 Groups as Foreign Terrorist Organizations, INTERPRETER RELEASES, Oct. 8, 2001.

11. Id. (explaining that the designation can be set aside based on five factors: 1) if the court finds the designation “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; 2) contrary to constitutional right, power, privilege, or immunity; 3) in excess of statutory jurisdiction, authority, or limitation, or short of statutory right; 4) lacking substantial support in the administrative record taken as a whole or in classified information submitted to the court under I.N.A.’s 219(b)(2) [8 U.S.C.A. § 1189(b)(2)], not in accordance with the procedures required by law”).

12. Id. (noting however that the court can review the fact that the organization is “foreign” or “engaged in terrorist activities”).

13. EI-Ayouty, supra note 4, at 485.

14. Id.

15. Id.

16. Id.

17. Id. at 486 (noting that this relationship provided for some form of compromise between the parties).
“freedom fighters” and once peace returned many were elevated to diplomatic posts or other political positions.\textsuperscript{18}

This terrorism, however, is not today’s terrorism. Today, there are no borders, no fronts, no clear ideology, no state, no government, and no physical structure.\textsuperscript{19} Rockets are no longer the weapon of choice, today it is either chemical, biological, or even nuclear weapons which can cause mass terror and sweeping destruction.\textsuperscript{20} This also leaves open the notion of cyber warfare against computers and telecommunication networks.\textsuperscript{21} As means of communication have evolved and expanded terrorists can see the “fruits of their labor” in seconds as images are broadcast throughout the world.\textsuperscript{22} Today’s terrorists are also interested in pseudo-religious and transcontinental objectives.\textsuperscript{23} Taken as a whole, this all looks depressing but what is worse is that many of today’s terrorists were “trained” by the United States.\textsuperscript{24}

C. Statistics

A misconception about terrorists is that they are on suicide missions. According to Center Intelligence Agency (CIA) statistics, 62\% of terrorists actually have a back up plan or escape route if things go wrong.\textsuperscript{25} Another way to protect their life is to engage in actions like placing a bomb or an assassination instead of hijacking an airliner or seizing official buildings.\textsuperscript{26} Terrorists even go as far as analyzing the likelihood of confronting the authorities before they engage in certain acts.\textsuperscript{27} Once terrorists have received the attention of the authorities they may even appear unselfish.

\textsuperscript{18} El-Ayouty, \textit{supra} note 4.
\textsuperscript{19} \textit{Id.} at 486 (recognizing that today’s terrorists have globalized, there is no longer an organizational chart, or fixed bases).
\textsuperscript{20} \textit{Id.}
\textsuperscript{21} \textit{Id.}
\textsuperscript{22} Higgins, \textit{supra} note 1, at 5.
\textsuperscript{23} El-Ayouty, \textit{supra} note 4, at 486.
\textsuperscript{24} \textit{Id.} (noting that individuals like Saddam Hussein and Osama bin Laden were “greenhoused” and “cocooned by the United States and/or allies of the United States like Pakistan, Saudi Arabia, Egypt, and Afghanistan when it was under Soviet occupation” as a way to prevent communist expansion into Afghanistan).
\textsuperscript{25} Higgins, \textit{supra} note 1, at 5 (illustrating that terrorists are not interested in losing their life as a result of their actions).
\textsuperscript{26} \textit{Id.}
\textsuperscript{27} \textit{Id.} at 6 (noting that other factors taken into consideration consist of risk and time).
because when they plead their case it is not personal; rather it is addressing something they believe should be changed.28

Terrorism is a concept that has evolved along with society.29 According to the United States Department of State, between 1968 and 1982, there were almost 8,000 terrorist attacks.30 However, 1985 was the record year for international terrorism with 800 deaths and 1,200 injuries.31 In the mid-1990’s there were on average two terrorist attacks a day, which varies between 600 and 850 per year.32 Another source, the North Atlantic Treaty Organization (NATO) Assembly’s Assessment of International Terrorism in 1987, reported that between the years of 1973 and 1983, 5,175 terrorist attacks were conducted killing 3,689 individuals while injuring 7,791 others.33 In 1997, 221 people died and another 690 were injured the entire year, however the following year these statistics were blown out of the water in a single one day, August 7, 1998.34

D. A Global Response

Leaders and nations from around the world have all spoken out against terrorism. In 1998, United Nations Secretary-General Kofi Annan was quoted as saying, “Terrorism is a global menace, which clearly calls for global action. Individual actions by Member States, whether aimed at State or non-State actors, cannot in themselves provide a solution. We must meet this threat together.”35 At this same conference, the Foreign Minister of Egypt described terrorism as “an international crime against all societies.”36 President Clinton was even quoted as saying “it is a grave misconception to see terrorism as only, or even mostly, an American

28. Id. at 150.
29. See text accompanying app. 1.
30. Higgins, supra note 1, at 4 (admitting that 188 terrorist groups carried out attacks on 3,162 victims of which 20% were either killed or wounded which included 540 international hostage-takings). See also, Yonah Alexander, Terrorism in the Twenty-First Century: Threats and Responses, 12 DEPAUL BUS. L.J. 59, 75 (1999/2000) (noting that in 1970 there were 300 terrorist attacks but by 1999 that figure had jumped to over 5,000 attacks).
31. Higgins, supra note 1, at 261 n.8.
32. Id. at 4 (noting that the majority of these attacks are concentrated in the United States and Western Europe).
33. Id. at 261 n. 8 (noting further that with every subsequent year the number of deaths increase by 20% with Europe alone suffering half of that).
34. Alexander, supra note 30, at 76 (referring to when 260 people were killed and another 5,000 were injured after the simultaneous bombings of the United States embassies in Kenya and Tanzania, supposedly masterminded by Osama bin Laden).
35. El-Ayouty, supra note 4, at 496.
36. Id.
problem."\textsuperscript{37} Kuwait declared that "it supports all collective international efforts to confront this phenomenon."\textsuperscript{38} The United Arab Emirates has also spoken out against terrorism claiming that "combating this dangerous phenomenon should not be carried out on a unilateral basis."\textsuperscript{39} Yemen has also stressed that "terrorism has become an international phenomenon. It concerns all nations and peoples, and there is a pressing need for the international community to respond immediately."\textsuperscript{40} Saudi Arabia's Chief Delegate has stated that, "[v]iolence and terrorism are universal phenomena rather than the characteristics of a certain people, race or religion. Precisely because of the comprehensiveness and universality of terrorism, the only way to combat it is through a unified and collective international action, within the framework of the United Nation."\textsuperscript{41}

Terrorism is a global phenomenon\textsuperscript{42} and it is the responsibility of the entire world to combat its efforts. There are numerous ways in which one can try and deal with terrorism.\textsuperscript{43} For example, more security has been added at airports where for years terrorists were able to come and go freely with material that should not have been able to leave the nation of origin.\textsuperscript{44} As previously illustrated, world leaders are beginning to make public statements denouncing terrorism and drawing attention to the brutal nature of terrorist attacks.\textsuperscript{45} Advances in technology have also allowed intelligence agencies to be better equipped to deal with potential attacks.\textsuperscript{46}

\begin{footnotes}
\item[37.] Id.
\item[38.] Id. at 497.
\item[39.] Id.
\item[40.] El-Ayouty, supra note 4.
\item[41.] Id. at 498.
\item[42.] Jacqueline Ann Carberry, Terrorism: A Global Phenomenon Mandating a Unified International Response, 6 IND. J. GLOBAL LEGAL STUD. 685, 686 (1999) (indicating that there are three factors that lead to terrorism being viewed as a global issue: 1. It "is not restricted to any one region, State, or jurisdiction," 2. "the increased mobility of terrorists to cross borders, acquire resources in numerous States, and access advanced communication systems," 3. The victims of terrorist attacks are not necessarily even members of the same State).
\item[43.] Alexander, supra note 30, at 89 (listing several options as publicizing it, improving intelligence gathering regarding it, enacting legislation, strengthening penalties against terrorists, and providing greater protection for facilities and officials).
\item[44.] Id.
\item[45.] Id. (illustrating that world leaders have used specific attacks to show the pointless nature of these instances).
\item[46.] Id. (noting that this has resulted from timely collection, analysis, and dissemination of relevant information on individual terrorists, their beliefs, means of operation, and other relevant information).
\end{footnotes}
For example, in 1991, European intelligence officials were able to prevent Iraqi initiated terrorism in connection with the Gulf War.\textsuperscript{47}

Changes in pre-existing laws have also aided in combating terrorism. The problem though is that laws are not consistent. The United States is a great example of this. Since states are free to define offenses through their criminal and penal code, terrorism can be defined fifty different ways. Take Arkansas for a definitional example, it's criminal code states, "a person commits the offense of terrorist threatening if with the purpose of terrorizing another person, he threatens to cause death or serious physical injury or substantial property damage to another person."\textsuperscript{48} There are nine general categories that terrorism falls under in United States' state law.\textsuperscript{49}

State law is not the only ambiguity that exists in the United States when it comes to a working definition of terrorism. For the past thirty years, Congress has held numerous hearings, proposed bills, adopted various resolutions, and passed a number of laws and yet there is still not a concrete definition on what constitutes terrorism.\textsuperscript{50} However, recently Congress has been trying to pass the "long arm statute that makes it a federal crime for a terrorist to threaten, detain, seize, injure, or kill an American abroad."\textsuperscript{51} In the 1980's the Federal Bureau of Investigation drafted an interagency definition of terrorism.\textsuperscript{52} However, the United States Department of State went ahead and drafted their own definition contained in Title 22 of the United States Code Section 2656f(d).\textsuperscript{53}

Following the Oklahoma City bombing, Congress was finally able to push through terrorism legislation in both the House of Representatives and

\textsuperscript{47} Id.
\textsuperscript{48} Alexander, supra note 30.
\textsuperscript{49} Id. at 61 (listing them as: civil defense, antiterrorism provisions, destructive devices, terrorist threats, enhanced criminal penalties, victim compensation, street terrorism, ecological terrorism and taxes).
\textsuperscript{50} Id. at 62.
\textsuperscript{51} Id. at 90.
\textsuperscript{52} Id. at 62 (stating it as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives").
\textsuperscript{53} Alexander, supra note at 30, 62-63 (defining terrorism as a "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience." The Code goes on to state that international terrorism is "terrorism involving citizens of the territory of more than one country," while a terrorist group is "any group practicing, or that has significant subgroups that practice international terrorism").
the Senate. President Clinton signed the Anti-Terrorism and Effective Death Penalty Act (AEDPA) of 1996 on April 24. In 1996, legislation was also passed allowing United States citizens who were victims of terrorism to sue the country responsible as long as it was listed on the United States Department of State’s list of nations who support terrorism. A few years later, Congress passed another bill taking things a step further by allowing these same individuals to tap the frozen assets of the countries they sued in order to receive their judgement. The Preparedness Against Terrorism Act of 2000 H.R. 4210, plans on implementing changes to existing laws to improve federal coordination and enhance domestic preparedness regarding terrorist attacks. Also, Presidential Decision Directive (PDD-62): Protection Against Unconventional Threats to the Homeland and Americans Overseas reaffirmed PDD-39: United States Counterterrorism Policy and expanded upon the use of weapons of mass destruction and cyber warfare.

Other nations and organizations around the world have their own definition of terrorism and have struggled with how to combat the problem. The United Nations has experienced difficulty when it comes to trying to define terrorism. In December of 1999, the General Assembly adopted a draft of the International Convention for the Suppression of the Financing of Terrorism that includes a working definition of terrorism.

54. Carberry, supra note 42, at 689 (noting that the Comprehensive Terrorism Prevention Act of 1995 was passed in the Senate on June 7, 1995 while the House passed their own version, the Effective Death Penalty and Public Safety Act of 1996, on March 14).

55. Id. (indicating that the bill sets aside one billion dollars over the next four years to numerous antiterrorism programs, it requires violators to make restitution to their victims, strengthens immigration laws preventing individuals believed to belong to terrorist organizations from legally entering the United States, increases the government’s power to deport foreigners convicted of crimes, and mandates that plastic explosives contain chemical taggants for tracking).


57. Id. (quoting Republican Senator Connie Mack of Florida, “the message is clear to terrorist nations: There is a price to pay for killing Americans”).

58. Charles L. Cragin, Terrorism Preparedness, Congressional Testimony by Federal Document Clearing House, May 4, 2000. (Noting that the Department of Defense’s role “is to be prepared to provide, when requested, available military forces and capabilities to support domestic requirements specified by the Attorney General of the United States or the Director of the Federal Emergency Management Agency”).

59. Id.

60. Alexander, supra note 30, at 64 (defining terrorism as “criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstances unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious, or other nature, that may be invoked to justify them”).
Over the years, the United Kingdom has implemented a few definitions of terrorism, some broad while others were narrower in scope. In 1996, Lord Lloyd's working definition of terrorism was "the use of serious violence against persons or property, or the threat to use such violence, to intimidate or coerce a government, the public, or any section of the public, in order to promote political, social, or ideological objectives." The latest definition of terrorism in the United Kingdom however, is the use or threat, for purposes of advancing a political, religious, or ideological course of action which involves serious violence against any person or property, endangers the life of any person, or creates a serious risk to the health or safety of the public or a section of the public.

Based on their definition of terrorism, the United Kingdom has implemented their own legislation. For the most part their terrorism legislation has tended to focus on the clash between Catholic and Protestant populations. The European Court of Human Rights however, does not approve of the United Kingdom's antiterrorism legislation claiming that the United Kingdom's seven-day holding period violates the European Convention on Human Rights. In 1989, the United Kingdom passed the Prevention of Terrorism Act, basically a reincarnated version of the Act of 1984, that banned any form of financial assistance to terrorists and gave the Secretary of State the power to exclude people thought to be involved in terrorism without court review and empowered the police to arrest an individual without a warrant if the officer reasonably suspected involvement in acts of terrorism. More recently the United Kingdom passed the Criminal Justice (Terrorism and Conspiracy) Act of 1998.

61. Id. at 63 (noting however that under the 1999 Prevention of Terrorism Bill the House of Lords wanted a broader definition of terrorism that would include expressions of single-issue extremism by groups).

62. Id.

63. Carberry, supra note 42, at 691 (citing the United Kingdom Prevention of Terrorism Act of 1984 that "proscribed the Irish Republican Army and the Irish national Liberation Army by placing the powers of detention, arrest, and exclusion in the hands of the Executive, designated that contributing to acts of terrorists as a crime and provided the police with the authority to conduct security checks on travelers").

64. Id. at 692 (noting that the government did not alter their law, "The government maintained that the seven-day period was essential and that the sensitivity of the information on which detention was based rendered its presentation to a court in the presence of the detainee impossible").

65. Id. at 693.

66. Id. at 694 (indicating its significance in the fact that it makes it easier to secure the conviction of terrorists, makes it illegal to conspire in the United Kingdom to commit a crime in
Throughout the world there are numerous treaties and conventions that address the act of terrorism.\textsuperscript{67} The New York Convention "mandates cooperation in preventing attacks on diplomats both inside and outside their territories, open exchange of information regarding the circumstances of the crime and the alleged suspect's identity, and coordination of administrative efforts against such attacks."\textsuperscript{68} The Hostage Convention also mandates that a State extradite or prosecute an individual believed to be involved in a terrorist attack.\textsuperscript{69}

There are several Conventions that specifically address the issue of hijackings. The Tokyo Convention is one such agreement.\textsuperscript{70} The Hague Convention, like the Tokyo one, is ambiguous when it comes to the definition of hijacking however.\textsuperscript{71} The Montreal Convention however did broaden the occasions when the offense of a hijacking could occur.\textsuperscript{72} Despite the fact that nations may actually be a signatory to a particular Convention does not mean they will adhere to its provisions. Take Uganda for example, back in 1976, it was a part of the Entebbe hijacking episode even though it had signed various hijacking Conventions.\textsuperscript{73}

Besides Conventions there are also several international conferences that have been held to address terrorism. At the Ministerial Conference on Terrorism on July 30, 1996 the G-8\textsuperscript{4} leaders adopted twenty-five practical antiterrorism resolutions.\textsuperscript{75} In 1985, the United Nations General Assembly

\begin{itemize}
\item \textsuperscript{67} El-Ayouty, \textit{supra} note 4, at 492 (comprising a list of the "Hijacking Convention of 1971, the Sabotage Convention of 1971, the Internationally Protected Persons Convention of 1973, the Hostage Convention of 1979, and the Maritime Terrorism Convention of 1988").
\item \textsuperscript{68} Carberry, \textit{supra} note 42, at 701 (noting that the State in actual possession of the offender must take measures to extradite or prosecute the individual and to notify other nations of action taken and/or submit all relevant evidence to assist in prosecutorial proceedings if conducted elsewhere).
\item \textsuperscript{69} \textit{Id.} at 702 (indicating however that this convention has been seriously weakened as a result of subsequent additions that allow nations to avoid extradition or prosecution).
\item \textsuperscript{70} \textit{Id.} (stating that an individual can be convicted of a criminal offense even if on board a flight outside of the borders of the contracting State).
\item \textsuperscript{71} \textit{Id.} (defining a hijacking as the "use of physical force, threat, or intimidation to take control of an aircraft as elements of hijacking").
\item \textsuperscript{72} \textit{Id.} (pointing out that a hijacking can occur even if the doors of the aircraft are not closed and the perpetrator is not currently present).
\item \textsuperscript{73} Carberry, \textit{supra} note 42, at 703 (acknowledging that despite its known involvement Uganda was never formally punished or censured).
\item \textsuperscript{74} Canada, the United States, Great Britain, Germany, France, Italy, Japan, and Russia.
\item \textsuperscript{75} Carberry, \textit{supra} note 42, at 704 (citing the resolutions: increased public transportation security measures, implementing global standards for detecting bombs, tightening border
adopted resolution No. 40/61, calling on all nations to “fulfill their obligations under international law to refrain from organizing, instigating, assisting, or participating in terrorist acts in other states, or acquiescing in activities within their territory directed toward the commission of such acts.” As a side-note, not one of the anti-terrorist conventions provide for either economic or other sanctions against States assisting terrorism.

E. National Responses to Terrorism

Around the world nations are facing internal terrorism. Many nations are quietly appeasing terrorism, or trying to contain it, while others have even become a terrorist’s haven. There is no consistency when it comes to terrorism but there are common threads that form a terrorist pattern that people can be aware of. The differences that emerge between terrorists will depend on their motivation and capabilities. Governments have used terrorists and their techniques to injure or topple foreign governments. The Soviet Union was also a sponsor of the Palestinian Liberation Organization (PLO) in the 1960’s 1980’s and maintained an extremely close military relationship. Another nation to engage in state sponsored terrorism is that of Iran. Approximately $300 million is given annually to the Hezbollah, along with organizational support, logistical and operational assistance. However, Iran claims that they do not sponsor terrorism, rather they [Iran] “only give political backing and humanitarian

controls, policing the Internet, improving exchange of intelligence information and drafting a treaty compelling countries to prosecute or extradite suspected bombers).

76. El-Ayouty, supra note 4, at 493 (citing a comment by Professor Oscar Schachter, “the condemnation of international terrorism thus imposes an obligation on all states to take appropriate measures to prevent acts of international terrorism. When suspected terrorists are apprehended the State must either extradite or try and punish them. This obligation, I believe, is now general customary international law”).

77. Id.

78. Id. at 494.

79. Alexander, supra note 30, at 68 (noting that smaller terrorist groups will tend to focus on bombings while larger organizations will tend to implement more complex operations, including kidnappings, assassinations, facility attacks, and hijacking).

80. Id. at 68 (acknowledging that the Soviet Union and other communist states engaged in this type of behavior during the Cold War).

81. Id. (suggesting that the PLO received money, training, and supplies from the Soviet Union that allowed them to engage in advanced operations against the Israelis over the years, specifically the Black September attack on athletes at the Munich Olympic games in 1972).

82. “Party of G-d,” an umbrella organization of radical fundamentalist Shiite groups dedicated to establishing an Islamic Republic in Lebanon.

83. Alexander, supra note 30, at 69 (recognizing that all this aid is used to fight “Western imperialism” in the Middle East along with removing the “Zionist” entity from the region).
aid to the groups."

Hezbollah also receives assistance from Syria. This financial assistance has allowed the organization to kill close to 130 people while injuring another 440.

The United States has also recognized the nations of Afghanistan, Cuba, Iraq, Libya, North Korea, and the Sudan to be nations that sponsor terrorism. Afghanistan is one of the worst nations when it comes to state sponsored terrorism. They have maintained training camps for members of the Harkat ul Majahideen. This group was responsible for the December 24, 1999 hijacking of India Airline’s Flight 814 from Nepal to Pakistan. The Harkat ul Majahideen is not the only terrorist group that Afghanistan assists. Internationally, their worst terrorist offense is their assistance of Osama bin Laden and the al-Qaeda network. Osama bin Laden is seen as a threat because of his views regarding the liberation of Saudi Arabia and Palestine along with the overthrowing of “corrupt” western-oriented governments in predominately Muslim nations. His operations have been widespread and destructive since the mid-1990’s.


85. Alexander, supra note 30, at 69 (providing a channel between Iran and the organization that also provides locations to mount their attacks against the nation of Israel through Syrian controlled areas in Lebanon).

86. Id. (recognizing that the Hezbollah was responsible for car bombings of the United States Embassy and Marine Headquarters in Beirut in 1983, kidnapping of numerous hostages in Lebanon in the 1980’s, rocket attacks on settlements in Israel proper in the 1990’s, destruction of the Israeli Embassy in Buenos Aires in 1992, and destruction of the office building housing the Argentine Jewry in 1994).

87. Id. at 70 (noting that these nations provide a safehaven, funding, training, and arms to various terrorist organizations around the world).

88. An Islamic terrorist group based in Pakistan and dedicated to liberating India’s Kashmir.

89. Alexander, supra note 30, at 70 (explaining that the plane carrying 178 passengers and eleven crew members was diverted to Afghanistan where the seize ended when the terrorists coerced India into releasing three jailed comrades, one of whom had declared a Jihad (holy war) against the United States and India).

90. Id. at 71 (noting that along with the Sudan, Afghanistan has been assisting possibly the worst terrorist organization in the world).

91. Id. (citing the fact that Osama bin Laden maintains formal and informal ties with terrorist groups in Algeria, Bosnia, Canada, Chechnya, Egypt, Eritrea, France, Libya, Pakistan, Philippines, Somalia, United Kingdom, United States, and Yemen as a way to achieve his goals).

92. Id. at 72 (indicating that he has been held responsible for the 1993 bombing of the World Trade center in New York City, the 1996 attack in Saudi Arabia of the Khobar Towers, and the 1998 bombings in Kenya and Tanzania at the United States’ Embassies). See also, Phil Hirschkorn and Deborah Feyerick, Ex-copilot pilot can’t link bin Laden to Somalia, CNN, Apr. 23, 2001, available at CNN.com/Law Center; see also Phil Hirschkorn, Scant Evidence Shown to link bin Laden to GI deaths in Somalia, CNN, Apr. 20, 2001, available at CNN.com/Law
In response to state sponsored terrorism there are several things that a nation may do. This includes adjusting their level of diplomacy with the specific nation in question, along with the possibility of economic sanctions, altering the level of law enforcement, and possibly the movement of military power. A nation is allowed to expel diplomats thought to be involved in terrorism. Economic sanctions are a hard measure to adhere to since they require international cooperation in many instances.

However, not all nations are adding to the problem of terrorism; many of them are actually helping to prevent its escalation. Today, nations are beginning to work collectively to bring terrorists to court to stand trial for their actions. Fawaz Younis was arrested during a FBI sting in international waters off of the coast of Cyprus and was eventually tried, convicted and sentenced for his crimes. If it were not for the assistance of Pakistan in 1995, Ramzi Yousef may still be at large. Besides extraditing terrorists, world governments are addressing the threats of terrorism by increasing security measures, like adding x-ray machines at airports around the world.

F. Terrorism’s New Threats

A new threat of international terrorism however is the stock piling of weapons. Many terrorist organizations are now trying to gain access to

---

93. Alexander, supra note 30, at 91.
94. Id. (pointing to the fact that the United States and many Western European nations have expelled Libyan diplomats over the years thought to be involved in terrorist activities).
95. Id. (recognizing however that the United States has successfully imposed sanctions against Iran and Libya while the United Nations has done the same against Afghanistan).
96. Id. at 90. He is a Lebanese operative from the 1985 hijacking of a Jordanian airliner that included American hostages.
97. Id.
98. Alexander, supra note 30 (noting that he was arrested in Pakistan and extradited to the United States for trial). See also, Carberry, supra note 42, at 689 (commenting that Abdul Hakeem was also extradited to the United States to stand trial for his involvement in the Philippine air case April 12, 1995 along with Ishmail Najim in August from Jordan for his involvement in the World Trade Center bombing).
99. Id. at 90 (noting that embassies are now built with added security measures in mind along with training sessions on how to deal with various terrorist threats).
100. Id. at 91 (admitting that they are not fool proof but effective none the less).
When its leaders were arrested after the Sarin gas attack in Japan back in 1995 the organization, Aum Shinrikyo, was actively seeking lethal weapons. People should be concerned about this because if a nuclear bomb was to get into the wrong hands an explosion of one kiloton anywhere could cause more than 100,000 fatalities and damage totaling billions of dollars.

When trying to combat terrorism people need to consider the socio-economic causes like poverty, hopelessness, and the non-observance of human rights driving young people into the arms of terrorism where "they find communal support, an identity and a cause through which they vent their anger through the heinous crime of terror." For an economist, to eradicate terrorism one must alter the benefits and cost structures to the point where peace is the most viable and optimal solution. Terrorism is not something that is going to vanish anytime soon. There are numerous causes that will continue to fuel its existence and unfortunately its expansion. Terrorism may be impacted by the growing xenophobia around the world directed against immigrants, refugees, asylum seekers, guest workers, and other "undesired" foreigners. New laws, stricter security or enforcement measures, and military strikes may actually prove counterproductive and result in the escalation of terrorism instead of reduction. Another factor that may lead to terrorism's growth is that of heightened goals among terrorists.

Around the world there are various forms of terrorism. One is that of biological terrorism. "Future terrorists wishing to wreak mass casualties

101. Id. at 72 (acknowledging that Osama bin Laden is trying to acquire biological, chemical, and nuclear weapons to use in subsequent attacks).

102. Id. at 63 (indicating that this Japanese doomsday cult had killed twelve and injured over five thousand with the release of the Sarin gas on the Tokyo subway). See also, The Anthrax Threat, THE ECONOMIST, Oct. 26, 2001, (pointing out that the intention was to kill thousands). Despite spending thirty million the cult could not produce the Sarin gas in a pure enough form, could not develop an effective delivery mechanism or distribution system.

103. Alexander, supra note 30, at 77 (noting that this would be only one-twentieth of the power released in the Hiroshima attack).

104. El-Ayouty, supra note 4, at 497.

105. Higgins, supra note 1, at 4.

106. Alexander, supra note 30, at 78 (noting that terrorism will also grow as a result of the publicity that is generated from attacks, the fact that arms, explosives, supplies, financing, and secret communication are all readily available, and international support networks exist that underwrite the activities).

107. Id. at 79 (noting that some terrorist organizations may actually try more defiant types of terrorism as a result).

108. Id. at 80 (eluding to the fact that as goals increase so to will terrorism because ideological and political violence is often seen as the means to an end).
may well turn to biological weapons." This results from the fact that as biotechnologies proliferate it is making it easier for state and non-state actors to develop weapons relatively easily and cheaply. A second form of terrorism is chemical in nature. The first instance of chemical terrorism occurred all the way back in 1915 when Germany released liquid chlorine from pressurized cylinders, allowing the poisonous gas to drift over enemy lines. Chemical and biological terrorism has been beneficial for terrorists because of their lost cost, ease and speed of production, along with the notion that people of limited education and facilities can develop them. Nuclear Terrorism is also a possibility. It is growing in use as well with the advent of nuclear bombs and fissionable material. Non-nuclear attacks are likely as well with radio-frequency capabilities.

III. THE NEWEST FORM OF TERRORISM

A. A Descriptive Analysis

The newest form of terrorism to emerge is that of cyberterrorism and information warfare to manipulate computer systems to disrupt or incapacitate infrastructures. This type of attack is the focus of the


110. Id. (acknowledging that many of the same technologies that go into fermenting beer can be used to manufacture biological weapons).


112. Id. at 82 (suggesting that this is the case because these weapons can be purchased without raising much suspicion and the space needed to build them is minimal).

113. Saxton, supra note 109 (maintaining that the theft or sale of such weapons is likely with lax security and possible monetary gain).

114. Alexander, supra note 30, at 82 (opining that for now nuclear terrorism will occur only as a credible threat or hoax involving a nuclear device, holding for political or economic blackmail a nuclear facility, or the bombing of a nuclear reactor site itself).

115. Saxton, supra note 109 (indicating that the United States’ electronic infrastructure could be damaged by such attacks).

116. Alexander, supra note 30, at 84 (defining information warfare to consist “of a broad spectrum of threats ranging from electronic jamming to psychological operations underscoring the perpetrators’ deliberate exploitation of military and civilian information systems’ inherent vulnerabilities and thereby adversely affecting national and global security” quoting the author of the article).

117. Saxton, supra note 109.
remainder of this paper. Many believe cyberterrorism\textsuperscript{118} began as something just for fun, but evolved into industrial espionage and eventually culminated in political motives.\textsuperscript{119} Cyberterrorists can be individuals, criminal organizations, dissident groups or factions, or even another nation.\textsuperscript{120} The reason cyberterrorism is growing so fast is because of how easy it is to launch a cyberattack. All one has to do is infect one computer and then allow it to pass through a network, infecting other machines or the entire network based on the program launched.\textsuperscript{121} The only tools needed to launch such an attack are a computer, modem, telephone, and hacker software.\textsuperscript{122}

The cyberworld has developed a language all its own when it comes to cybercrime. At one point it was very simple, the good guys were Hackers while the bad guys were Crackers. Today everyone involved in cybercrime is identified as a Hacker,\textsuperscript{123} those with an interest in the workings of a computer.\textsuperscript{124} "Hackers" are individuals with a certain code of ethics; they do not damage systems or data and are good programmers.\textsuperscript{125} However, there are some hackers who are beginning to emerge lacking this code of ethics.\textsuperscript{126} "Crackers,"\textsuperscript{127} on the other hand, are not bound by any ethics; they break into systems with malicious intent or

\textsuperscript{118} See generally, Cybercrimes: Infrastructure Threats From Cyber-Terrorists, 2 CYBERSPACE LAWYER 23, (1999) (defining cyberterrorism as "the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives").

\textsuperscript{119} Vijay Mukhi, Internet Instructor/Political Hacking, THE TIMES OF INDIA, Nov. 8, 2000, available at 2000 WL 28353566 (stating that at first it was just to acquire credit card numbers, and then it evolved to companies illegally accessing customer and product information from the other). See also Cybercrimes, supra note 118, at 23.

\textsuperscript{120} Cybercrimes, supra note 118, at 23 (noting that attacks can be internal or external and may be directed against a computer system, or focus on the infrastructure itself).

\textsuperscript{121} Mukhi, supra note 119, (noting that once a system is infected it can send out the IP (Internet Protocol) address of your computer to a machine anywhere around the world or send out its own code as an e-mail attachment and then trigger itself once the attachment is opened).

\textsuperscript{122} Cybercrimes, supra note 118, at 23.

\textsuperscript{123} Mukhi, supra note 119.


\textsuperscript{125} Id. (noting that their activities are both productive and creative). See generally, Jennifer McKee, Hackers of a Different COLOR, ALBUQUERQUE J., Feb. 11, 2001 (acknowledging that they tend to be older individuals who are gainfully employed and educated).

\textsuperscript{126} Ching, supra note 124 (indicating that these individuals are being called Black Hat Hackers while those who maintain the code of ethics are beginning to be referred to as White Hat Hackers).

\textsuperscript{127} McKee, supra note 125 (analyzing that the term derived from people "cracking" into websites or software copyrights).
strictly for money while destroying both data and systems.128 Below Crackers are “Script Kiddies,” individuals who buy or download “scripts” that will search the Internet for crackable sites129 “Hactivists”130 are computer hackers with political and social agendas.131 While “cybervandals” are individuals who’s actions alter information on spreading dogma on political and social sites.132 “Denial of service”133 refers to attacks that overwhelm a computer’s ability to handle incoming messages.134 “Defacers” are those who “deface” a website or system.135 “Defacements” are a common cracker prank and include WebPages that crackers post over with pre-existing websites that they have cracked.136 While a “Patch” refers to computer codes that can be used to fill in security gaps left by crackers when they broke into the website.137 “Trojan Horses” are programs that appear to perform a useful function and sometimes do so quite well but also includes an unadvertised feature, which is usually malicious in nature.138

128. Ching, supra note 124 (acknowledging that these individuals rarely write their own programs and their efforts are completely destructive in nature).

129. McKee, supra note 125 (labeling them the “ultimate poseurs” and calling them the “lowest form of code tweekers” according to Codeflux.com, a hacker website that publishes a “jargon dictionary”).

130. Naomi Koppel, Anti-globalist Protesters Turn to Hacking to Thwart Opponents, THE CANADIAN PRESS, Feb. 8, 2001, available at 2001 WL 12573165 (recognizing that the term was first applied to Zapatista supporting rebels in Mexico’s southern state of Chiapas who held virtual sit-ins and sabotaged Mexican government websites since 1998).


132. Auerbach, supra note 131, at 23.

133. Bruce Sterling, Revenge of the Smurfs, THE WALL ST. J. EUR., Feb. 16, 2000, at 10 (suggesting that this term along with “distributed coordinated attacks” may be replaced with “Smurfing.” Further noting that it is not a big deal, no security is broken, firewalls are not melted down, no data is stolen, instead it just jams up the works; thus it is cheap, quick, dirty, and highly effective).

134. Auerbach, supra note 131, at 23.

135. McKee, supra note 125 (noting that sometimes these individuals will even provide links to sites that will correct the problem or links to the actual website that they have “defaced”).

136. Id.

137. Id.

138. Cybercrimes, supra note 118, at 23.
B. The Growth of Cyberterrorism

There are many factors, which seem to be operating, that allow for cybercrime both internally and externally according to Raja Azrina Raja Othman, the MyCert project head. Cyberterrorism seems to be the new way to wreak havoc around the world. "The World's growing dependence on the Internet opened the door to renegade individuals and states who could cripple economies and inflict death by remote control." The threats of cyberattacks grow with every passing day. There are three basic reasons for this. The first reason is the international growth of the Internet itself, which causes "policing" to be much more difficult. Secondly, there are already over 30,000 hacker-oriented websites, which makes it extremely easy for people to acquire the knowledge necessary to disrupt or destroy whatever they are seeking. And finally, with the end of the Cold War came a mass exodus of terrorist organizations to other locations around the world making it difficult to track them.

The reason that cyberterrorism is seen as so problematic is because an attack could come from anyone or anywhere and could take any form. Hypothetically speaking, an organization with a budget of say ten million with thirty computer experts strategically located throughout the world could bring the United States to its knees with a well-coordinated cyberattack. "Computer networks will increasingly be the main

139. Ching, supra note 124 (listing the internal factors as: "Lack of control and poor management in computer administration;" "lack of knowledge and exposure in aspects of computer security;" "low priority given by top management;" "poor or haphazard computer network and system design that is unsafe, ill-equipped with security components, and misconfigured systems and application," outdated software and lack of maintenance." The external factors cited include: "Free exploit tools or programs available over the Internet;" "Vulnerable computer systems and application," "Motivation . . . to establish status quo or for monetary gain," and "Lack of ethics and professionalism among budding technologists").

140. Richard Ingham, Cyberterrorism: Death, Ruin at a Touch of the Return Key, AGENCE FRANCE-PRESSE, May 16, 2000 (QUOTING FOREIGN MINISTER YOHEI KONO AT the conference on cybercrime at the G8 (Group of Eight) meeting).

141. Alexander, supra note 30, at 86 (estimating that there are already 120 million users and there will be close to a billion by 2005).

142. Id. (indicating that these sites contain information on step-by-step instructions, Trojan horses, and logic bombs).

143. Id.

144. Ingham, supra note 140 (noting that an attack could result from a single assailant, a group or government holding cheap equipment and knowledge pertaining to the Internet's structure).

145. Cybercrimes: supra note 118, at 23 (listing thirteen possible forms that a cyberterrorist attack could take).

146. Alexander, supra note 30, at 86.
battleground for armies and terrorists. Computers are the roads and bridges of the Information age . . . the most important targets for people or organizations bent on disabling communications. It’s a basic military tenet . . . [t]ry to shut down your enemy’s infrastructure.”

C. Cyberterrorism’s Impact and Coverage

Right now cyberwar is emerging as the “third largest threat” to developed nations behind chemical and bacteriological attack and nuclear weapons.” Every week more than fifty computer viruses are released. Also, every week a new computer hacker cracks into Pentagon computers or breaks into the databases of banks or other financial institutions. It has even been reported that over $400 million in financial losses resulted from cyberattacks in 2000, up 40% since 1999. In 1999, it has been reported that the United States had $12.1 billion dollars in damage caused by Internet viruses with the Melissa virus costing close to $10 billion across the world. It is believed that only 25% of wired companies are secure. Currently, it is believed that close to 80% of all foreign attacks on United States computers either originated in or passed through Canada. This is believed to be the case because Canada is such a wired nation. Recently, in Edmonton and Calgary “Hacking Schools” were

147. Auerbach, supra note 131, at 23 (quoting Stanton McCandlish of the San Francisco privacy and civil liberties group Electronic Frontier Foundation).
148. Ingham, supra note 140 (referring to a comment made by Colin Rose of Buchanan International, a Scottish-based company specializing in tracking Internet offenders. He went on to say “The potential for harm is enormous. If you can destroy industries and essential services with the touch of a button, you don’t need to bother with bombs”).
150. Id.
154. Martin Stone, Canada Called Hotbed of Cyberterrorism, NEWSBYTE NEWS NETWORK, Mar. 27, 2000 (relying on an American intelligence agency determination).
155. Id. (indicating that “the high number of hacker attacks coming from Canada is due to a high degree of computerization . . . Canada is a very wired country and that hackers will typically bounce through different computer systems to hide their original location.” Colonel Randy Alward).
established to address the issue of cyberattacks. The cost of a training session can range from $500 all the way up to $5,000. China, on the other hand, is looking to establish similar schools with the exact opposite intention.

Currently, cyberattacks are mounting around the world. It is believed that political cyberterrorism has been around since 1998 as far as web defacement and denial of service attacks are concerned. But cyberattacks may go back as far as 1986, when West German hackers stole passwords, programs, and other data for the KGB. The United States' Pentagon systems and a nuclear weapons lab were among several targets for an Israeli hacker in February of 1998. This past New Year's Eve there was also a conspiracy plot to take down the Internet.

China has been involved in many cyberattacks on both sides. Two years ago, after the accidental bombing of the Chinese Embassy in Belgrade, China "retaliated" electronically. In China, as military tensions have risen, there have been reciprocal attacks on computer networks between the mainland and Taiwan. It has been estimated that Taiwan's governmental network has been broken into over 150 times with a report suggesting that over 72,000 attacks have been launched against

---

156. Monchuk, supra note 153 (differentiating kids who want to learn how to be a hacker from companies who are signing up employees to learn how to build a defense).
157. Id. (recognizing that the more expensive course is much more in-depth).
158. Frank J. Cilluffo et al., Bad Guys and Good Stuff: When and Where will the Cyber Threats Converge?, 12 DEPAUL BUS. L.J. 131, 151, (1999/2000) (claiming that China wants to train "cyberwarriors" at Army schools to wage war over the Internet and eventually establish a fourth branch in their military devoted to Information Warfare).
159. Elinor Abreu, Chinese Hackers are Blamed for Vandalizing U.S. Websites, Apr. 13, 2001, available at Thestandard.com/article/0,1902,23717,00.html (providing that this first attack seems to have been from a British hacker who published anti-nuclear messages on about 300 websites).
160. Alexander, supra note 30, at 84 (noting that this was accomplished after they broke into military, scientific, and industry computers in the United States, Western Europe, and Japan).
161. Id. (indicating that Ehud Tenenbaum and two other young collaborators from California engaged in the cyberattacks).
163. Cilluffo, supra note 158, at 151 (referring to the cyber activity that they engaged in which revealed close to 4,000 back doors," allowing outsiders to regain access to programs at a future date, into United States computer systems).
164. Auerbach, supra note 131, at 23. See also, Cilluffo, supra note 158, at 153 (indicating that the cyberattacks resulted from Taiwan's President Lee Teng-hui stating that there should be relations between the two nations as equals).
Another incident linked to China has been the e-mail bombs that have proliferated the Chinese spiritual group Falun Dafa's website. China is also under investigation for the defacement of nine United State websites as a possible retaliatory measure after one of their fighter jets was downed in early April.

The North Atlantic Treaty Organizations' (NATO) website along with other government related sites have been bombarded with electronic mail and hit with antiwar rhetoric. Since the start of the Al Aqsa Intifada between Israel and Palestine no permanent damage has resulted from their cyberwar campaign. So far it seems that this type of cyberterror has only been used to raise awareness pertaining to each side's cause. In fact, the virus that was released contained a note indicating that no damage would result. An issue not quiet addressed yet however is the public's perception of such attacks.

People should not believe that the United States is immune from involvement. There are rumors that the United States spent more money trying to cripple Iraq "invisibly" during the Gulf War than we spent on military hardware. There are also rumors that President Clinton

165. Cilluffo, supra note 158, at 153 (according to Pentagon estimates the spreading of two Taiwanese viruses have caused $120 million in damage and damaged 360,000 computers in China).

166. Auerbach, supra note 131, at 23 (suggesting that China was responsible because at the time China was engaged in cracking down on this group while a British agency was able to track transmissions that seemed to originate from XinAn Information Service Center in Beijing, thought to be a subsidiary of the Chinese Ministry of Public Security).

167. Abreu, supra note 159.

168. Auerbach, supra note 131, at 23 (indicating that the attacks might have originated from activists connected with the Serbian side of the Balkan conflict). See also Alexander, supra note 30, at 85 (calling these attacks "Aping attacks" because of the way that they establish communication with a target computer and then occupy its functions by continuously staying linked and "feeding" it information). See also Cilluffo, supra note 158, at 149 (suggesting that a group called Crna Ruka [Black Hand] could be responsible because they had attacked the Kosovo Information Center the previous year).

169. Pro-Israel Hackers Told to Ignore 'Cyberterror,' HA'ARETZ, Mar. 23, 2001 (citing that there was a pro-Palestinian e-mail virus that struck 10,000 Israeli e-mail users).

170. Id. (noting however that things could get out of hand if one side decided to up the anty).

171. Id. (indicating that the attacks so far have been superficial, mainly defacing websites as opposed to damaging infrastructures that could cause huge economic damage).

172. Id. (suggesting according to Yael Shahar, Webmaster at the International Policy Institute for Counter Terrorism at the Interdisciplinary Center, Herzliya that "many groups on both sides have realized that hacking, while intended to create 'public relations' for their cause, is actually viewed by the public as criminal activity").

173. Ingham, supra note 140 (according to Colin Rose).
authorized a plan to destabilize Slovodan Milosevic by employing hackers to disrupt his foreign bank accounts.174

D. New Weapons and their Impact on Cyberterrorism

Its not just cyberattacks that are alarming nations but what terrorists are using personal computers for. As technology advances, many terrorist organizations have gone online. For example, the Hezbollah maintain a daily record of “heroic” battles carried out by its fighters in Southern Lebanon on its official website.175 Besides website propaganda, terrorists are using their personal computers to store information pertaining to their plans for future attacks.176 It is even believed that Osama bin Laden’s organization is maintained through satellite "uplinks" and encrypted messages that they pass back and forth through their computers.177 According to United States officials, encryption has become the “everyday tool of Muslim extremists.”178

Currently, there are new weapons at the disposal of cyberterrorists. They are no longer limited to just computers. In corporate “spec wars” cyberterrorists have begun using Magnetic Pulsing Devices that erase data up to 100 yards without leaving any trace or evidence of their users.179 Another weapon at the disposal of cyberterrorists besides a computer is a HERF gun; it can destroy a server from thirty yards away.180 The gun works by changing all the 0s and 1s into only 0s leaving permanent damage in which none of the effected data can be recovered.181

174. Cilluffo, supra note 158, at 150 (noting that there was also a suggestion that the United States was planning an attack on the Yugoslav command-and-control network along with the air defense system).

175. Alexander, supra note 30, at 87 (noting that Afghanistan now publishes its radical form of Islam on the Internet as well).

176. Id. (indicating that Ramzi Ahmed Yousef had plans on his personal computer to blow up several American airlines over the Pacific Ocean, he is currently in jail for his role in the World Trade center bombings).

177. Id. See also Jack Kelley, Terrorists Use Web to Mount Attacks, THE ARIZ. REPUBLIC, Feb. 6, 2001, at A9 (estimating that encryption has enabled Osama bin Laden to carry out his three latest plots).

178. Id. (recognizing that “Uncrackable encryption is allowing terrorists Hamas, Hezbollah, al-Qaeda, and others - to communicate about their criminal intention without fear of outside intrusion.” FBI Director Louis Freeh at a closed door Senate testimony panel on terrorism last March).

179. Patrick Sweeney, Be Aware of Off-Site Storage Security, 38 COMM. NEWS, Feb. 1, 2001, at 76 (pointing out that this weapon is small enough to fit inside a cigarette carton making it almost impossible to track into the office).

180. Id. (noting that the weapon can be made easily by anyone for less than $600).

181. Id.
E. What's Being Done to Deal with the Problem

It may be hard to address the problems raised by cyberterrorism because politically motivated attacks can be difficult to investigate or prosecute. That does not mean nothing is being done to address the problem. The Department of Justice and the Federal Bureau of Investigation in 1998 formed a new unit called The National Infrastructure Protection Center to address cyberterrorism issues. The Department of Justice has also established an internal Computer Crime and Intellectual Property Section (CCIPS) to address international computer crimes.

These are not the only things the United States government has done in an effort to eliminate cyberterrorism. President Clinton outlined four cyberterrorism initiatives in 1999 during a speech that he delivered at the National Academy of Sciences. And then last year, he announced further initiatives to counter the evolving problem of cyberterrorism. One suggestion was offering college scholarships to individuals who studied computer security in return for their public service upon graduation.

We need to do more to bring people into the field of computer security. That's why I am proposing a new program that will offer college scholarships to students in the field of computer security in exchange for their public service afterward. This program will create a new

---

182. Abreu, supra note 159 (indicating the thoughts of Michael Vatis, the director of the Institute for Security Technology Studies at Dartmouth College. "[A]nytime you have political tension in the world, it's being mirrored by attacks in cyberspace").

183. Auerbach, supra note 131, at 23 (indicating that the unit was established to strengthen the United States' defenses against cyberterrorism and other electronic threats). See also Tom Spring, Cybervandalism is Tough to Thwart, PC WORLD ONLINE, Feb. 9, 2000, at 2000 WL 8855770 (hi-lighting that malicious hackers could be fined upwards of $250,000 and/or between five and ten years in jail).

184. Bruce Braun et al., WWW.CommercialTerrorism.com: A Proposed Federal Criminal Statue Addressing the Solicitation of commercial Terrorism through the Internet, 37 Harv. J. 159, 177 (2000) (citing the Department of Justice website indicating that the goal of the section is for "government officials ... the private sector ... academic institutions, and foreign representatives to develop a global response to cyberattacks").

185. Jon Baumgarten et al., Clinton Attacks Cyberterrorism, 1 CYBERSPACE LAW. 16, (1999) (outlining the four initiatives as follows: A Critical Infrastructure Applied Research Initiative, tasked with detecting various activities or codes; Computer Intrusion Detection Networks which will evaluate and design networks to detect attacks and warn other systems; Information Sharing and Analysis Centers established to encourage private-sector development along with providing outreach and training programs, and finally. Cyber Corps to set-up scholarships and financial aid programs).

generation of computer security specialists who will work to defend our nation’s computers.187

Another initiative involved a $2 billion package to counter cyberterrorism by securing the nation’s computer systems.188 Included in this plan would be an increase in governmental funding for research and development, establishing a ROTC-type corps of information technology specialists and forging a new partnership with the private sector.189 President Clinton was also interested in establishing The Institute for Information Infrastructure to “fill research gaps that neither public nor private sectors are filling today.”190 The House Energy and Commerce Subcommittee on Oversight and Investigations have also scheduled hearings to discuss how vulnerable the United States is to cyberattack.191

California seems to be paving the way of cracking down on cyberattacks within their state. California Governor Gray Davis signed a bill introduced by Assemblyman Rico Oller, R-California, which raises the fines for first-time offenders from $250 - $1,000 as long as no harm resulted from their access to computers or unauthorized domain name offenses.192 Under the new law, first-time hackers who do not cause damage by introducing a new virus could face a fine of $5,000 or one year in jail.193

Current federal criminal laws that have been used to address Internet crime have included laws against mail and wire fraud, the federal riot act, consumer protection acts, commerce protection acts, and statutes prohibiting the issuance of threats and solicitations of violent crimes.194

190. Transcript, supra note 187 (quoting President Clinton again at the news conference on the South Lawn at 9:28 a.m. EST indicating that the Institute would “bring to bear the finest computer scientists and engineers from the private sector, from universities and from other research facilities to find ways to close these gaps”).
192. Ronna Abramson, California Cracks Down on Cyberterrorism, THE INDUSTRY STANDARD, Sept. 28, 2000 available at www.TheStandard.com/article/o,1902,18961,00.htm (explaining that this also raised the violation from an infraction to a misdemeanor).
193. Id. (noting that second-time offenders could face $10,000 and up to three years in a state prison if their action results in harm).
194. Braun, supra note 184, at 164-65 (noting that despite the laws being on the books for decades many of them were not enacted with Internet activity in mind and thus do not correctly apply to the problem).
Because these laws do not specifically address the problem of Internet terrorism some academics from Harvard College have decided to draft a proposed statute. The authors of this statute, Bruce Braun, Dane Drobny, and Douglas C. Gessner, President and Fellows of Harvard College, believe that as things stand currently, the Internet resembles the "lawless Wild West." The authors further pointed out, that the United States Justice Department has done little to track down and prosecute Internet terrorists. For purposes of their statute they have defined "commercial terrorism as the unlawful use of force or violence against persons or property to intimidate or coerce commercial interests."

The first section of their proposed legislation includes the definitions for "Internet," "Interactive computer service," and "Information content provider." Part II of the draft addresses "Online solicitation to commit a crime of violence." Here they lay out the punishment for those who "transmit[s] or cause[s] to be transmitted via the Internet or interactive computer service in interstate or foreign commerce any communication containing any demand or request that another person engage in conduct constituting a felony in violation of state law or the laws of the United States." Many provisions of their proposed legislation are based on existing federal legislation that has been altered to encompass Internet related crimes. There are potential problems with this legislation when it comes to enforcement however. The Internet has allowed for anonymity. A terrorist can easily hide his/her identity and if the prosecution cannot

195. Id. at 159.
196. Id. at 160 (describing the Internet as being "open to governance by human instincts, including those of greed, deception, and hate").
197. Id. (noting that even if the Justice Department made prosecution of Internet terrorists a top priority little could be done because of current laws, they are either "too broad, too cumbersome, or fail to address the type of destruction caused by Internet terrorism").
198. Id.
199. Braun, supra note 184, at 169-70 (acknowledging that these definitions "parrot" the Communications Decency Act, 47 U.S.C. § 230(e) (1994), and were not struck down by a recent Supreme Court decision based on this provision).
200. Id. at 169-70.
201. Id. at 170 (setting forth the possibility of an affirmative defense if the defendant is able to thwart the commission of the crime that was solicited or prove that they were not a party to the commission of the crime but were rather used as an unknown conduit for dissemination of the information. However, the statute further notes that it is not a defense to claim that one is immune from prosecution).
202. Id. at 171 (noting that certain provisions are based on 18 U.S.C. § 373 (1994)).
track him/her down then there is no case.\textsuperscript{203} As a result, for successful enforcement, the authors suggest that the federal government work in conjunction with academics, the private sector, and the Internet community.\textsuperscript{204} However, this cyber-manhunt\textsuperscript{205} is not impossible.\textsuperscript{206}

The United States is not the only nation to begin to address the concerns surrounding cyberterrorism. Japan has also begun to implement strategies to counter the threat after learning how vulnerable they are. It seems that Japan is an easy target for cyberterrorism because many of its leaders are computer illiterate when it comes to understanding computer networks or the threats they face.\textsuperscript{207} "Until those attacks, very few people in the government, business, or the media had even heard of cyberterrorism."\textsuperscript{208} In February of last year, Japan implemented a law allowing for the prosecution of hackers as a result of worldwide pressure.\textsuperscript{209} A network will be established that links the Ground Self-Defense Force, the Maritime Self-Defense Force and the Air Self-Defense Force, along with construction of integrated information and communication networks that include an anti-cyberterrorism unit.\textsuperscript{210} This unit will be designed to monitor the agency's networks and to protect its data.\textsuperscript{211} Other areas covered include a guarantee of the interoperability of this network with the

\textsuperscript{203} Id. at 174 (describing the difference that occurs in a "typical" criminal act in which eyewitnesses or written documentation can 'be gathered as opposed to an Internet terrorists' "ability to remain anonymous").

\textsuperscript{204} Braun, supra note 184, at 175 (opining that this is the best method for three reasons. First, the expertise or technology are within the private sector or academic world. Second, as Internet consultants emerge on the screen they are going to have to work with law enforcement officers. And finally, due to the size of the Internet, a centralized government enforcement would be ineffective).

\textsuperscript{205} Id.

\textsuperscript{206} Id. at 176 (pointing out that a lot of Internet terrorists will not try to conceal their identity making it easy to find and prosecute them. Also, the federal government has resources that could be transferred to this type of endeavor).


\textsuperscript{208} Id. (quoting Raisuke Miyawake, a former government official referring to attacks successfully launched by hackers who attacked Japanese government websites criticizing them for trying to "whitewash" its military record during World War II).

\textsuperscript{209} Id. (expressing that "[o]ther industrialized countries have had to urge Japan to strengthen its legislative defenses against cyberterrorism" according to Mr. Miyawake).


\textsuperscript{211} Id.
United States military in Japan and for research into what IT developments will do to military technology.\footnote{212}

The Liberal Democratic Party (LDP) has established a task force to address the issue, seeking a special command office, a team of specialists devoted to cybercrimes, the need to strengthen computer security systems, and nurturing experts to combat cybercrime.\footnote{213} The LDP came up with a proposal suggesting that the nation strengthen website security and related systems, including a two-stage schedule of how to accomplish this and indicated that a board of government officials and cybercrime experts from the private sector should be established.\footnote{214}

Like California in the United States, Malaysia seems to be the pioneer in the East when it comes to combating cyberattack. Hacking has been illegal in Malaysia since 1997.\footnote{215} However, that has not stopped the problem. In the first eight months of 1999, Malaysia had forty-seven cases of website hacking while in the previous year they only had twenty-eight.\footnote{216}

\section*{F. Critics of the Importance Placed on Cyberterrorism}

Despite world concern, there are individuals who do not see cyberterrorism as a valid issue at all.

Look, nobody died. When a site is down, there may be some lost business. But look at all the problems we have over the registration of guns. People die as a result of guns. Maybe the government should be paying a little more attention to weapons that actually kill people.\footnote{217}

Mr. Bridges went on to state, "I don't think cyberterrorism is going to accomplish anybody's death. Recipes have been on the Internet for a long time. The problem is all these words with 'cyber'-prefixes are ways to create jingoist alarmism."\footnote{218} Joel de la Garza of the security firm

\begin{footnotes}
\footnote{212}{Id.}
\footnote{213}{\textit{LDP Task Force Outlines to Combat Cyberterror}, THE YOMIURI SHIMBUN / DAILY YOMIURI (ASIA), Feb. 10, 2000, available at 2000 WL 4642972 (noting that the task force was established as a result of attacks by hackers on ministry and agency Web sites).}
\footnote{214}{Id. (recommending in the long term a law on high-net crimes and a campaign to educate the public on proper and improper usage of the Internet).}
\footnote{215}{Ching, supra note 124 (referring to section 5 of the Computer Crimes Act of 1997 indicating that a penalty of RM100,000 can be fined or jail time up to seven years).}
\footnote{216}{Id.}
\footnote{218}{Id. (quoting Andrew Bridges).}
\end{footnotes}
Securify argues that many web defacements are "just a bunch of kids performing the cyber equivalent of toilet-papering someone's house."²¹⁹

But who is really hurt by cyberterrorism? Think about it,

"[i]t would cost the average Bangladeshi more than eight years' income to buy a computer, whereas it would cost the average American just one month's wage. . . . [a]nd what would this repository of information, in which more than 80% of the content is in English, mean to 90% of people worldwide who do not speak it."²²⁰

IV. CONCLUSIONS

Terrorism is not new; however, today it is different than it has been in the past. The same elements may still be present, but new ones have emerged that add to the threat. Terrorism began as "freedom fighters" fighting for their liberation, self-termination, or social/political cause. It has evolved to be a political weapon. Whenever an individual has an issue, instead of taking the legal means to solve it he/she turns to terrorism and destroys lives and property. What does this honestly solve? Nothing.

In the earlier days of terrorism, one could expect a suicide mission, a car bomb, or hijacking. Today, the sky is the limit. With terrorists amassing great fortunes of wealth and the ability to acquire weapons of mass destruction, there is no telling what today's terrorists will try. Actually, weapons are not even needed anymore. Today, with a computer, terrorists can accomplish almost anything. What is worse is that cyberterrorism is sure not to be the final version of terrorism. Just as terrorism evolved from hijackings, bombs, and suicide missions to chemical, biological, or even nuclear means, cyberterrorism seems to be the next step in this evolving terrorist arsenal and who knows what the world will be facing.

But for now, the world needs to concern themselves with the implications of cyberterrorism and be ready for any situation that occurs. To do this effectively is going to require a global commitment and right now that does not seem to be the case. Despite the fact that world leaders and nations have come out against terrorism, there are still places in the world that provide a safe haven for these individuals and organizations and as long as these places exist, terrorism will survive.

²¹⁹. Abreu, supra note 159 (noting that this is not as serious as other cyber attacks that could be waged).

²²⁰. Supra note 152 (quoting Deputy Prime Minister Datuk Seri Abdullah Ahmad Badawi).
V. ADDENDUM

Since this paper was written a lot has changed in the world but this section is going to focus on the events of September 11th. I think that one would be hard pressed to find an individual who anticipated the events of September 11th. Most people in this country, actually in the world for that matter, never expected someone to attack the mainland of the United States because many thought that the United States was indestructible. That is no longer the case. Everyone is beginning to understand that the United States is just as vulnerable as any other nation in the world. As a result, a lot of security measures have been implemented and terrorism is beginning to be taken more seriously by everyone.

Let us begin with the new anti-terrorism legislation, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, that passed Congress with enormous speed. The goal of this legislation is to deter and punish terrorist acts in the United States and abroad. The USA Patriot Act of 2001, as it is also known, will achieve its goals through law enforcement’s and intelligence agencies’ expanded roles. These organizations have been authorized to expand telephone tapping, monitoring of Internet traffic and conducting other surveillance in pursuit of terrorists. This bill also includes provisions to combat money laundering. Another new measure provided for in this legislation is expanded information sharing among agencies, including allowing the FBI to have access to private records. The bill also extends the statute of limitations for terrorist acts while strengthening

221. Bill to Combat Terrorism Contains Money Laundering Provisions: USA Act of 2001, ANDREWS' BANK & LENDER LIABILITY LITIG. REP., Oct. 18, 2001. See also Legislative Activity Veers Toward Border Control, Scrutiny of Aliens, INTERPRETER RELEASES, Oct. 1, 2001, at 5 (listing several other goals of this legislation as “strengthening domestic security, updating and enhancing surveillance procedures, stopping financial support for terrorists, tightening security along the Canadian border, providing for greater criminal history information sharing with the State Department and the INS, removing personnel obstacles to investigating terrorism, protecting victims of terrorism, increasing information sharing for critical infrastructure protection, strengthening criminal laws against terrorism, and regulating biological weapons”).


223. Bill to Combat Terrorism Contains Money Laundering Provisions: supra note 221 (noting that this applies to private banking and correspondent banking by United States financial institutions on behalf of offshore banks and foreign nationals).


penalties for those who assist terrorists. In addition to this, immigrants suspected of terrorism or aiding terrorism can be detained for up to a week without being formally charged or deported for simply raising money for a terrorist organization. At the last minute, another provision was inserted that would require all schools to report on the status of their foreign students.

This legislation also creates a counterterrorism fund in the Treasury Department to reimburse “the Justice Department for the cost of countering, investigating and prosecuting domestic or international terrorism.” The bill also extends the period in which electronic surveillance can be performed on a non-United States person along with roving surveillance on telephones used by suspected terrorists. A final provision would allow the government to detain suspected terrorists for seven days without bringing formal criminal or immigration charges.

This bill did not receive unanimous approval. In the Senate, Senator Russell Feingold (D-Wis.) voted against the measure. His biggest contention against the bill was the secrecy of searches and surveillance. Not all of the provisions were hailed as breakthroughs in the fight against terrorism. Many organizations voice opposition based on civil liberties, specifically privacy and individual rights. David Cole, an expert on Constitutional law teaching at the Georgetown University Law Center, believes that this legislation is simply too “sweeping.” Mr. Cole fears that law-abiding non-citizens will be deported simply because of “guilt by association.” He went on to state his reservation to the provision allowing the attorney general to place immigrants in custody based on

226. Id.
227. McFeatters, supra note 225.
230. Id.
231. Id.
232. Robert E. Pierre, Wisconsin Senator Emerges as a Maverick; Feingold, Who Did Not Back Anti-Terrorism Bill, Says He Just Votes His Conscience, THE WASH. POST, Oct. 27, 2001, at A8 (acknowledging that he originally supported the Attorney General’s position but had to change his mind because he feels that the legislation takes away too many freedoms).
234. Id.
235. Id.
suspicion without an ounce of evidence.\textsuperscript{236} There has also been criticism expressed by privacy groups who believe that this legislation provides too much power to the government to monitor online communications.\textsuperscript{237}

President Bush responded to this criticism by saying that "the bill protects, rather than erodes, civil liberties by increasing federal authorities' ability to prevent, rather than just respond to terrorist attacks."

\textsuperscript{238} A sunset provision was also included in the bill to appease civil liberties organizations, providing an expiration of 2004 for many of the major provisions and dictating that the Justice Department prepares a report of how civil liberties are impacted.\textsuperscript{239} Professor Jesse Choper, a Constitutional Law Professor at the University of California at Berkeley, points out that the federal government has every right to pull back individual rights to protect national security interests.\textsuperscript{240}

Another bill to pass both Houses of Congress quickly was the anti-money-laundering bill. This was passed after President Bush froze the assets of an original twenty-seven individuals and organizations and another thirty-nine suspected accounts.\textsuperscript{241} One of the reasons it is so important to freeze assets, is that an organization or individual does not have the means to execute their plan.\textsuperscript{242} This bill contains three main provisions. First, the United States Treasury Department would gain the power to single out foreign countries or banks suspected of money laundering. Second, the securities industry would be required to report suspicious transactions, and finally it would be illegal to bring more than

\textsuperscript{236} Id.

\textsuperscript{237} Id. (noting that these groups are also afraid that grand jury secrecy rules would be loosened while restrictions on searches would be eased as well).

\textsuperscript{238} McFeatters, supra note 224.

\textsuperscript{239} McFeatters, supra note 225 (establishing a way to also sue the government if personal data is disclosed in a harmful manner).


\textsuperscript{241} The Money Trial, THE ECONOMIST, Oct. 26, 2001. Along with freezing the assets of individuals and organizations President Bush's plan also authorized the freezing of assets belonging to banks that do business with terrorists and those who did not cooperate with the American probe. See also Manuel Perez-Rivas, Investigators making progress in 'worldwide puzzle', Oct. 2, 2001, available at www.cnn.com/2001/us/10/02/inv.investigation.status/index.html (indicating that over $6 million dollars of terrorist accounts have been frozen, including thirty al-Qaeda accounts in the United States and an additional twenty overseas). See also Money Laundering: Japan Freezes $750,000 in assets of Taliban, Affiliates, Ministry Says, INT'L BUS. & FIN. DAILY, Oct. 23, 2001. (pointing out that Japan has frozen $750,000 assets contained in thirty-one deposit accounts thought to belong to the Taliban and affiliated individuals and organizations).

\textsuperscript{242} The Money Trial, supra note 241. (indicating that it is estimated that it only cost $200,000 to execute the September 11th attacks).
$10,000 cash into the United States. However, people acknowledge this bill may not be able to prevent Osama bin Laden from accessing his money. Money laundering normally involves dirty money, whereas he is able to engage in clean money.

The Keeping America Safe Act of 2001 focuses on aliens and how the United States government would deal with them post-September 11th. Rep. Robert E. Andrews (D-NJ) introduced legislation that would amend the Immigration and Naturalization Act (INA) § 212(a)(3)(B)(i)(IV)(V) and (iii)(IV)(V) to provide for “the inadmissibility of aliens who aid or abet a terrorist organization, including those designated as foreign terrorist organizations pursuant to INA § 219, or aid and abet an individual who has conducted, is conducting, or is planning to conduct a terrorist activity.”

Another act that focuses on aliens is the Criminal Alien Visa Denial Act of 2001, introduced by Rep. Christopher Shays (R-Conn.). This Act provides for a coordinated effort between the United States State Department and the INS to share access to United States criminal databases before an alien is allowed to enter the country. The interaction between the State Department and INS may be expanded with the passage of Senator Edward M. Kennedy’s (D-Mass.) bill. It would provide electronic access for both the State Department and INS to criminal history records held by the Federal Bureau of Investigation (FBI) to determine whether a visa applicant has a criminal history.

Besides being concerned with aliens, Congress has also been busy providing for the armed services. In a House defense authorization bill Congress allocated $343 billion to the armed services to help with border security.

243. Id.

244. Id. (describing dirty money as the proceeds from say drug trafficking going through the financial system as a way to make it look clean whereas clean money is harder to track because it normally consists of money that has been donated to a charity and later used for criminal endeavors).

245. Legislative Activity Veers Toward Border Control, Scrutiny of Aliens, INTERPRETER RELEASES, Oct. 1, 2001, at 1528 (acknowledging that the amendment would also amend § 237(a)(4)(B) to “provide for the deportation of those aliens deemed inadmissible under the new § 212(a)(3)(B)(i)”).

246. Id. (explaining the importance of this measure by citing an example of how an alien can enter the United States, commit a crime, leave, and get permission to reenter from the United States State Department without being detected because previously the State Department could not access the National Crime Information Center [hereinafter NCIC] database).

247. Id. (indicating that this would amend INS § 105 by making it easier to obtain these records, whereas in the past there were many regulations standing in the way of the information sharing requested).
Not everyone supported this legislation however. Reps. Solomon Ortiz (D-Tex.) and Silvestre Reyes (D-Tex.) opposed this amendment arguing that military training does not automatically equate to border patrol and that they are already understaffed. Rep. Sheila Jackson Lee (D-Tex.) also pointed out that this legislation might be unconstitutional because it allows military personnel to serve in a civil law enforcement capacity. Along with increased spending for defense, there is also a bill pending regarding aviation security. The bill seeks stationing federal marshals on flights, along with increasing cockpit security and training pilots to handle hijacking situations.

With Congress passing so much legislation President Bush has also asked them to push ratification of two treaties currently stalled in the Senate. The first is the International Convention for the Suppression of Terrorist Bombings, which would require prosecution, or extradition of any individual involved in a terrorist bombing within their jurisdiction. The second Convention is the International Convention for the Suppression of the Financing of Terrorism and refers to raising or collecting money to sponsor terrorist activities instead of bombings.

Besides legislation aimed at strengthening terrorism prevention there has also been the creation of various offices, agencies and task forces. One is the Office of Homeland Security. According to White House Spokesman Ari Fleischer, Tom Ridge is expected to "craft a coordinated, integrated and comprehensive national strategy to combat domestic terrorism." Mr. Ridge is expected to have complete authority over the planning process, and budget authority over federal terrorism and security.

---

248. *Id.* (noting that this is an amendment to the National Defense Authorization Act for Fiscal Year 2002 and put forward when it was discovered that some of the terrorists had entered the United States from Canada. "If 300,000 illegal immigrants trying to find a better life can gain access to America, do not believe for one moment that a larger contingent of people with evil intentions could not gain entry," Rep. Jim Traficant [D-Ohio], the one who introduced the amendment).

249. *Id.*

250. *Legislative Activity Veers Toward Border Control Scrutiny of Aliens, supra* note 245 (indicating that this may violate the posse comitatus prohibition of USC Title 10).


252. *Id.* (explaining that this Convention was signed January 1998 and sent to the Senate in September of 1999 where it still remains).


254. President Bush’s new Director to head up the White House Office of Homeland Security.

programs. In the beginning he needs to establish a clearinghouse in a secure location for monitoring terrorist activity and managing the government’s response in the event of an attack. However, this agency would not have military authority or intelligence gathering capabilities. There are some that believe establishing another office is not the answer. Instead of a coordinator some argue that a security Czar would be better.

The Combating Terrorism Technology Task Force (CTTTF) is another creation resulting from September 11th. This task force was established September 19, 2001 and is charged with developing an integrated plan to coordinate efforts in the field. Another group to be established was the Foreign Terrorist Asset Tracking Centre on September 14, 2001 charged with tracking terrorist finances. Along with tracking terrorist finances, President Bush wants to establish a Foreign Terrorist Tracking Force that would be assigned the role of tightening restrictions on immigration.

A task force like the above mentioned example, is needed to track foreigners as they enter this country. There are 300 checkpoints in which individuals can enter the United States. To illustrate the importance of tracking, take Ahmed Alghamdi for example. He was a student who legally entered the United States on a student visa but thereafter disappeared. INS had no idea where he was until September 11th when he hijacked a plane and crashed it into the south tower of the World Trade Center.

256. Id.
257. Id.
258. Id.
261. The Money Trial, supra note 241 (noting that this task force was actually created over a year ago but did not begin operations until after the September 11th attacks).
262. Tighten U.S. Immigration Rules, AP, Oct. 30, 2001. (indicating that the goal of the task force would be to coordinate with other federal agencies to prevent terrorists from entering the United States). See also Somini Sengupta, U.S. Doors Indefinitely Closed to Refugees, N.Y. TIMES SERVICE, Oct. 30, 2001. (indicating that the United States is not only watching immigrants but also refugees. Until further notice the borders will be closed to all refugees).
263. Gorman, supra note 228 (stating that United States borders are crossed 500 million times a year with thirty-one million nonimmigrant people crossing annually with three to four million visitors remaining after their visas have expired).
As a result of this there has been a call for national identification cards and automated entry and exit systems at all major border checkpoints. INS Commissioner James Ziglar has promised to unveil an automated entry-exit system at all United States airports by 2003.

When the United States decided to begin a campaign to eradicate the Taliban from Afghanistan and a counterterrorist offense against the al-Qaeda network President Bush declared that "either you are with us, or you are with the terrorists." It seems that many nations of the world heeded his declaration and have joined the battle. Even the internationally recognized President of Afghanistan, Burhanuddin Rabbani, has publicly supported President Bush's air strikes against his own nation. The first nation to side with the United States was Great Britain. Prime Minister Tony Blair has committed 200 Royal Marine commandos to standby on ships in the Indian Ocean with an additional 400 placed on "high readiness". Prime Minister Blair went on to state that the action was necessary to prevent Osama bin Laden from acquiring "chemical, biological, even nuclear weapons of mass destruction." Prime Minister John Howard of Australia has also pledged 1,500 defense personnel to join the United States in its war against Afghanistan. Germany has pledged

264. Id. (pointing out that nine of the other seventeen hijackers had valid visas while six are unaccounted for).

265. Id. (crediting the national ID card to Senator Feinstein (D-Calif.) and the border system to Senator Edward Kennedy (D-Mass.) and Senator Sam Brownback (R-Kan.)). Senators Kennedy and Brownback are also interested in making it harder to falsify or misuse immigration documents, establish a tracking system through the schools where these individuals are supposedly registered, and create a way for the State Department, INS, and intelligence agencies to share information about suspected terrorists.

266. Id.


268. Afghan President Supports Escalated Airstrikes, at CNN.com, (Oct. 27, 2001) (stating that this is the best way to eradicate terrorists).

269 Michael Dobbs, Afghanistan, WASH. POST SERVICE, Oct. 27, 2001, at A19. (indicating that this was "a huge responsibility" that was needed to "defend civilized values around the world."")

270. Id. (noting that "if they are allowed to carry on like this, our world will be an insecure, unsafe place, and there will be no corner of the world – particularly not a place like Britain – that will be untouched by that."")

an additional 35,000 troops for the "war against terrorism" while Canada has pledged six warships, six planes and a total of 2,000 personnel.

Although Great Britain was the first nation to provide assistance, the first world leader that President Bush spoke to was Russia's President Putin. There are several reasons why Russia would want to side with the United States. First, Russia does not want to see radical Islamic elements extend into Central Asia. Secondly, the United States along with the European Union have relaxed their opposition to Russia in criticism of their handling of Chechnya. However, there are several Russian military leaders who do not think that this cooperation is a good idea, arguing that Russia should be more concerned about Iraqi's security than the United States'. As a result, President Putin has stated that Russian airspace can only be used for humanitarian missions.

Since September 11th, Japan has undergone a remarkable transformation in military presence. As a result of World War II, Japan had severe restrictions as to what sort of military operations it could conduct. But that may all change very soon. At the end of October, Japan approved a measure authorizing Japanese military support to the United States led anti-terror campaign. This could pave the way for Japanese troops to be sent overseas, however, they would not be permitted to engage in combat. The legislation also allows the Japanese military to

272. Christoph Bluth, Germany Considers 'was on Terror Role, JANE'S INTELLIGENCE REV., Nov. 1, 2001, available at 2001 WL 10122422 (indicating that Special forces could also be sent).


274. Timothy J. Colton & Michael McFaul, America's Real Russian Allies, FOREIGN AFF., Nov. 1, 2001, at 46. (noting that many believe that Russia came to the United States' side so quickly as a way for President Putin to later link the United States' stand against terrorism with their own battle against Chechn rebels).

275. Makarenko and Biliouri, supra note 267.

276. Id.

277. Colton and McFaul, supra note 267 (recognizing however that the Russian people support the United States in part of a deep support of democracy).

278. Makarenko and Biliouri, supra note 267. (indicating that he believed the way to eradicate terrorism was by "tackling poverty, international conflicts and other problems that have been correlated with the rise of terrorist groups").

279. Parliament Authorizes Japan Support Troops, supra note 273; see also, Hans Greimel, Japan Passes Law to Join Terror War, LOS ANGELES TIMES, Oct. 29, 2001. (pointing out that Japan may begin transporting weapons and ammunition in the war against terror in the air or on the high seas but not on foreign soil).
guard United States bases on Japanese soil along with permitting their coast guard to fire on suspicious vessels.\footnote{Parliament Authorizes Japan Support Troops, supra note 273; see also, Greimel, supra note 279.}

Another country to pledge support to the campaign against terrorism has been China. Its President, Jiang Zemin, said that he condemns all terrorism and would support the United States' attack against Afghanistan and the Taliban as along as it was directed at military targets and not the Afghan people or Islam in particular.\footnote{John Hill, China Sides With USA, JANE'S INTELLIGENCE REV., Nov. 1, 2001, available at 2001 WL 10122415.} He went on to add that China and the United States, as major influences in the world, have a responsibility to protect peace and stability in the Asia-Pacific region and the world.\footnote{Id.}

There is speculation however that the attacks in Afghanistan could destabilize neighboring Central Asian States and make it easier for authoritarian rule to rise along with an increase in indigenous Islamic militance.\footnote{Id.}

The irony is that Central Asian States have been seeking Western support in their battle against terrorism and until September 11th their voices were ignored.\footnote{Id.} However, now they have a strategic advantage over the United States who could use their locations for President Bush's "sustained and relentless" terrorism campaign.\footnote{Id.}

Uzbekistan's President, Islam Karimov, has stated that he would cooperate "[i]f investigation[s] proves that the terror attacks had been prepared on the territory of Afghanistan," indicating that "there must be retribution."\footnote{Id.} The current state of dialogue between the two nations would allow the United States access to Uzbekistan airspace and airbases along with an exchange of intelligence.\footnote{Id.} In return for this concession, the United States has agreed to target Afghanistan training camps that trained members of the IMU (Islamic Movement of Uzbekistan).\footnote{Id.}

Tajikistan is also getting involved in the campaign to eradicate terrorism. Prior to September 11th, the President of Tajikistan, Imamali

\footnote{Id. (pointing out that these nations have been asking for help since the Islamic Movement of Uzbekistan (IMU) conducted its first wave of terrorism in Kyrgyzstan and Uzbekistan back in 1999).}

\footnote{Id. (recognizing that Uzbekistan would be an ideal nation to have on the United States' side because of its strategic location allowing for sustained attacks on terrorist training camps and Taliban installations within Afghanistan).}

\footnote{Id. (limiting its missions to humanitarian and search-and rescue operations).}

\footnote{Id.}

\footnote{Makarenko & Biliouri, supra note 267.}
Rakhmonov, had supported counterterrorism measures in the Commonwealth of Independent States and Central Asia, making it seem that he would join in the efforts of the United States.\textsuperscript{289} President Bush believes that Tajikistan could be beneficial in the campaign to arm the Taliban opposition by utilizing routes through the country that have been previously used by Russia and its allies to aid the Northern Alliance, the opposition force against the Taliban.\textsuperscript{290}

Lebanon is also supporting the anti-terrorism campaign. They have pledged their support and stationed additional troops at embassies and other interests of countries supporting the campaign.\textsuperscript{291} Along with additional troops, Lebanon has staged drills to practice for various hijacking situations.\textsuperscript{292} It is not just individual nations that are supporting the campaign against terrorism; there are also global organizations that are aiding in the effort. The Asia-Pacific Economic Cooperation Forum is one such organization.\textsuperscript{293} However, not all nations or organizations are in support of Operation Enduring Freedom. The only involvement that Iran will have in the campaign is to continue supplying the Northern Alliance because it does not support military retaliation by the United States.\textsuperscript{294}

Nations around the world are not just aiding the United States. They are also passing legislation back home to strengthen their own terrorism laws. Surprisingly this includes laws regarding cyberterrorism. The European Union (EU) in conjunction with the Council of Europe (COE) have proposed cybercrime legislation in an attempt to prevent the “misuse of the Internet.”\textsuperscript{295} The COE has also received support from all fifteen EU countries on the world’s first international agreement on crimes committed

\textsuperscript{289} Id. (acknowledging however that their support may be minimal and hidden due to the lack of border control and factionalism).

\textsuperscript{290} Id. (noting however that border issues have to be discussed because as the campaign against Afghanistan intensifies many refugees with be leaving Afghanistan via Tajikistan).


\textsuperscript{292} Id.

\textsuperscript{293} Regional Briefing, supra note 271 (acknowledging their statement condemning terrorism along with calling for heightened security for telecommunications and transport and promised “appropriate financial measures” to stop terrorist funding).

\textsuperscript{294} Makarenko & Biliouri, supra note 267 (noting that Iran believes that any terrorist campaign against Afghanistan should also include a war on drugs). See also U.S. Sees Broader Role in Columbia as Part of Anti-Terror Fights, Oct. 26, 2001 (pointing out that the United States’ war on terrorism has expanded beyond Afghanistan and Osama bin Laden. The United States has pledged counterterrorism aid to Colombia in addition to military aid to assist in their war on drugs).

in cyberspace. The Convention calls for the parties to "cooperate . . . to the widest extent possible" in investigation and prosecution of computer related offenses along with the "collection of electronic evidence of a criminal offense." Germany is also looking to pass local legislation that would make it easier to use informants in criminal prosecutions along with requiring fingerprints for passports and identity cards.

Since the September 11th attacks, attitudes towards money laundering have changed. The American government along with other nations and organizations now acknowledge the tracing of money and restricting its flow to terrorist groups are key elements in the war against terrorism. Following these attacks sixty-six countries have introduced legislation to block the assets of organizations identified by the United States as terrorist in nature. While many nations are strengthening their money laundering laws, Italy has actually become more lax with the passage of legislation making it more difficult to investigate cross-border financial flows.

It is not just nations that are looking at these laws, multinational organizations are also amending their provisions regarding money laundering. As a way to combat money laundering the Organization for Economic Cooperation and Development (OECD) held an emergency meeting to look at the financing of terrorist groups. The Basel Committee on Banking Supervision released previously prepared guidelines on the subject. The Asian-Pacific Economic Cooperation forum also indicated that it would tighten its money-laundering laws while the

296. Id. (referring to the agreement as the European Cybercrime Convention and also indicating that there might be problems passing the legislation if separate approval is required from the EU and national ratification).

297. Id. (listing offenses that must be criminalized – computer related forgery, computer-related fraud, content related offenses like child pornography on the Internet along with intellectual property right infringements).

298. Bluth, supra note 272 (noting that this was done after it was learned from FBI intelligence that many of the terrorists involved in the September 11th attacks had resided in Germany before coming to the United States for flight school).

299. The Money Trial, supra note 241.

300. Id. (acknowledging that the United Arab Emirates and Saudi Arabia are among the sixty-six nations, which is crucial because a lot of money that finances Osama bin Laden's al-Qaeda network is believed to have originated in these countries). See also, Money Laundering: France Moves to Freeze Financial Assets of Terrorist Organizations Listed by U.S., INT'L BUS. & FIN. DAILY, Sept. 27, 2001 (pointing out that France was the first nation to comply with President Bush's bid to curb the money flow by groups linked to the September attacks. Between September 11-26th France had frozen $3.9 million in bank accounts).

301. Id.

302. Id.

303. Id.
European Union indicated that it would broaden its efforts to prevent laundering earned or used in all serious crimes. The United Nations Security Council also passed a money-laundering provision.

Along with the money laundering legislation that Congress passed the United States has implemented Operation Green Quest to target underground money transfers. It will be housed in the United States Customs Service headquarters and staffed by financial crime investigators from the Treasury and Justice Departments. This operation will hopefully reveal new information on sources of terrorist funding and systems similar to hawala, a way to evade legal banking systems by transferring money from one source to another via different countries.

In the beginning, the operation is slated to focus on illicit charities, counterfeiting, credit card fraud, fraudulent export and import schemes, drug trafficking, and cash smuggling.

Many experts around the world believe that the events of September 11th were the work of Osama bin Laden and the al-Qaeda network. There is debate not only as to whether he is in fact the mastermind behind these attacks but also what should be done to him if he is in fact responsible. Some say that there should be no trial and he should just be killed as soon as he is apprehended. Others believe that he should be put on trial in the United States as a way to prove that the American system of justice can still function in times of adverse circumstances. But does anyone believe that any courtroom in the country could pull together an unbiased jury to try him?

304. Id.


307. Rob Garver, Terro-Fund ‘Quest’ From Treasury, AM. BANKER, Oct. 26, 2001, available at 2001 WL 26574662 (quoting Treasury Deputy Secretary Kenneth Dam as saying that the “operation’s objective is to ‘launch comprehensive investigations resulting in blocking orders, criminal prosecutions, civil and criminal forfeitures, and other actions’”).

308. Customs Service Goes After Terrorist Funding, supra note 306.

309. Id.


311. Id. (pointing out that this may not be the safest way to go because there is no guarantee that United States citizens would be safe in the same courtroom as Osama bin Laden).
The debate over a trial has emerged as a result of President Bush calling for Osama bin Laden's capture. Both United States and international law would call for a trial if he was in fact apprehended. If Osama bin Laden was tried in the United States, any city in which the flights originated could serve as proper venue along with where the flights crashed or even where the pilots trained or opened bank accounts. If however, it was decided that Osama bin Laden would be tried overseas, according to a hijacking convention adopted thirty years ago, he could be tried in any of the eighty nations who lost citizens in the attack. Some argue that an international trial would be more appropriate because of the international cooperation that exists to handle the situation. The United Nations Charter would provide another path. Chapter 7 provides the Security Council with authority to create special courts when peace and security are threatened. A problem with all of these solutions is that it provides Osama bin Laden with a public forum. Not only could he recruit more followers but also classified information could be revealed that would compromise United States intelligence sources. Osama bin Laden has spoken once publicly since the events of September 11th. He was quoted as saying that “America will not live in peace” unless the United States withdraws its troops—the army of infidels—from Saudi Arabia and ceases its support for Israel.

Prior to the attacks as previously indicated in this paper, Osama bin Laden has been known to keep in contact with his followers via satellite phones and the Internet. Intelligence reports foiled a Paris Embassy plot masterminded by one of Osama bin Laden’s cells. There it was determined that all communications regarding the plot were to be carried

312. Id. (indicating that if Osama bin Laden was captured and tried in the United States he could also be tried for the embassy bombings in Kenya and Tanzania were 224 people were killed and an additional 5,000 injured).

313. Id. (noting that there are persuasive arguments for trying Osama bin Laden in the United States. The attacks occurred on United States soil, violated numerous United States laws and most of the victims were United States citizens).

314. Id. (acknowledging that the Convention binds 175 signatory countries to prosecute hijackers and their accomplices or extradite them to countries that will).

315. Weinstein, supra note 310 (explaining that by trying Osama bin Laden in the United States it would “shift attention from the global nature of the attack” causing an “enormous” amount of “legitimacy, certainly in Muslim countries,” Anne-Marie Slaughter, a professor of International Law at Harvard University).

316. Id. (noting that this is what was done to investigate the war crimes in Yugoslavia).

317. Id. (indicating that a way to avoid this would be to try him in a closed military tribunal).

318. Id.
out via coded messages hidden in pictures on the Internet.\textsuperscript{319} However, since the September 11th attacks Osama bin Laden has been evading authorities by returning to "stone age" communication.\textsuperscript{320} Despite bin Laden’s return to the "Stone Age" it is still thought that his cells communicate via encrypted Internet messages.\textsuperscript{321} Even if an encrypted message is discovered, there is little that can be done unless the government has access to a supercomputer and then there is usually not enough time to decrypt it.\textsuperscript{322}

While Osama bin Laden may be going low-tech, the Federal Bureau of Investigation (FBI) is going high-tech. Since September 11th, the FBI has increased Internet surveillance and setup a website to monitor developments surrounding the plane attacks.\textsuperscript{323} However, despite the FBI’s increased cyber presence other federal agencies are scrutinizing their websites and removing any information that they believe would benefit a terrorist.\textsuperscript{324} No one is exactly sure what information is valuable but Attorney General Ashcroft pointed out that an individual in federal custody was discovered to have downloaded information on crop-dusting planes that could be used for biological or chemical attacks.\textsuperscript{325}

Early in October, a government antiterrorism commission recommended that a cybercourt be established to prosecute hackers.\textsuperscript{326} Governor Gilmore\textsuperscript{327} believes "[a] court dedicated to criminal cyber conduct can develop the needed expertise to act appropriately on investigative activities while ensuring the protection of civil rights and liberties."\textsuperscript{328} The court would sit in "secret" and possess special powers


\textsuperscript{321} Id. (noting that they use these methods to cover their tracks when sending e-mails and coordinating their movements).

\textsuperscript{322} Id.


\textsuperscript{324} Feds Remove Information From Web Sites, AP, Oct. 25, 2001.

\textsuperscript{325} Id.


\textsuperscript{327} Governor of Virginia and Chairman of the Commission.

\textsuperscript{328} Ramasastry. supra note 326.
regarding search and surveillance. This court would be modeled after the Foreign Intelligence Surveillance Act (FISA) court. Some believe that a cybercourt goes too far and argue that instead of establishing a new court we should allow the existing courts to do their jobs. Over the years, courts have taken existing laws and applied them to technological advancements and many believe that they could do the same thing here. An alternative suggestion would be to allow the existing FISA court to serve as the cybercourt as well since they both potentially involve national security issues.

Since the September 11th attacks the United States has also been hit with an outbreak of anthrax. There is still debate as to where the anthrax is coming from with experts taking sides, arguing that it was either domestic or foreign in nature. Almost all experts admit that there has not been a direct link to any foreign organization. Although there is a report of Osama bin Laden buying $10,000 worth of anthrax on the open market in Eastern Europe and South-East Asia. There is another report that his associates were able to obtain $3,685 worth of anthrax from a factory supplied to the Indonesian-based Islamic Moro Front.

Gerald Brown, a retired United States Air force anti-terrorism specialist believes that the anthrax is “homegrown.” However, there are also those who believe that the letters were written by people who are not familiar with the English language or are unfamiliar with American

329. Id.
330. Id. (acknowledging that this court consists of a rotating membership of United States federal district court judges). There has been a lot of criticism from civil rights organizations regarding this court because it conducts its proceedings in secret and does not have to adhere to traditional Fourth Amendment guarantees. The purpose of the court is to deal with government surveillance and reviews Justice Department’s requests for electronic surveillance and physical searches of individuals who are suspected to be national security risks. The point of contention is the fact that everything is done in secret, thus people would may not even know that their home was searched or their phone tapped. The defendant may not even have access to the reasons why they were subjected to a search and the resulting information may later be used in a criminal prosecution.

331. Id. (noting that judges have been able to apply the Fourth Amendment to global positioning devices and infrared heat sensors).
332. Id.
334. Id.
handwriting. Although, there is also a theory that the letters were in fact written by a native English-speaker who is just trying to focus suspicion elsewhere. Or it could even be an individual trying to be childlike in nature. There is some speculation that Iraq is behind the anthrax letters as well but there has been no definitive link to this theory. Anthrax is also beginning to appear outside of the United States. On October 11th, numerous letters were received in Germany claiming to contain anthrax spores and an indication that the "jihad" had begun. Brazil, Argentina, and the Bahamas have also reported anthrax-contaminated letters.

It is hard to know what is going to happen from here but I think that it is safe to assume that life will never return to pre-September 11th existence. Whether this means that there will be a renewed patriotism or people living constantly in fear, one thing is certain; nothing will be overlooked or believed not to be possible. Hopefully, we have seen the worst but chances are there is more to come. It is time to be prepared.

336. Id.
337. Id.
338. Id.