CYBERTERRORISM: ARE WE LEGALLY READY?

Aviv Cohen ∗

INTRODUCTION

Human beings, by their very nature, have a tendency to find the destructive side of most innovations and advancements. Current technological developments present us with opportunities to enrich our lives by using simple, quick and high-quality devices. At the same time, these technological developments also hold the potential to be used as weapons in the hands of terrorists. When I first became acquainted with the idea of cyberterrorism, I was fascinated by the large amount of ink that had already been spilled on the gloom prospects that cyberterrorism is not a question of "if" but of "when."

However, there was no reference as to how the international community can react to such an attack after it had happened. This article is an attempt to take that next step, and try to analyze whether the international tool kit is well equipped to handle cyberterrorism. I have focused on the legal aspects, rather than discussing the technological options to combat cyberterrorism. While existing counter-terror conventions could, by way of legal interpretation, apply to cyberterrorism, there could be a better direct way of addressing this threat, via the creation of an explicit regime for the suppression of cyberterrorism consisting of conventional prohibitions, Security Council resolutions and international criminal laws.

The article includes four parts. Part I sets the stage for the arguments presented above, and provides a brief introduction to the concept of terrorism and the international response to these terrorist threats. Part II defines what cyberterrorism is and what distinguishes it from other manifestations of terrorism. Part III examines international conventions that were designed to address certain types of terrorism and whether they would be applicable in cases of cyberterrorism. Finally, Part IV discusses several avenues to address cyberterrorism in the future.

∗ This Article is based on my LL.M. Thesis. I would like to thank Prof. Moshe Hirsch and Prof. Yuval Shany of the Law Faculty of the Hebrew University of Jerusalem for their insightful and inspiring notes. This article is dedicated to my parents, Netta and Amir Cohen.

I. INTERNATIONAL LEGAL RESPONSES TO TERRORISM

Almost every country in the world condemns terrorism and assigns itself to fight it, but what exactly are they fighting against?[1] Answering this question and distinguishing terrorist acts from non-terrorist acts forced states to crystallize definitions of terrorism. Defining the term "Terrorism," however, is not a simple task. Specialists in the area of terrorism studies have devoted hundreds of pages toward trying to develop a widely accepted definition of the term, only to realize that "terrorism is intended to be a matter of perception and is thus seen differently by different observers."[2]

The complexity of finding an agreeable definition for "Terrorism" is considered one of the obstacles in creating an international mechanism to combat it.[3] Terrorism is a subjective concept, associated with different events in the eyes of different groups of people. One thing remains clear – terrorism is commonly regarded as a destructive force threatening the world as we know it in a way that makes it nearly impossible to prevent.

The widely accepted definition for terrorism at the international level is found in Article 2 Section 1(b) of the United Nation ("UN") International Convention for the Suppression of the Financing of Terrorism, 1999 ("The Financing Convention").[4] This definition has been reaffirmed in other international instruments, such as in the UN Security Council Resolution 1566[5], and is widely accepted among scholars.[6] The Article reads as follows:

---

[1] Daniel Taub, *Terrorism in the International Law, in* INTERNATIONAL LAW 476, 476 (Robbie Sabel ed., 2003).

[2] Audrey Kurth Cronin, *Behind the Curve: Globalization and International Terrorism*, 27(3) INT'L SEC. 30, 32 (2002).

[3] MALCOLM N. SHAW, INTERNATIONAL LAW 1048 (5th ed. 2003).

[4] International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, 39 I.L.M. 270 (hereinafter "Financing Convention").

[5] S.C. Res. 1566, U.N. Doc. S/RES/1566 (Oct. 8, 2004):

> …Recalls that criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offenses within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations …

[6] Tim Stephens, *International Criminal law and the Response to International Terrorism*, 27(2) U. NEW SOUTH WALES L.J. 454, 461-462 (2004). *See also*: Reuven Young, *Defining Terrorism: The Evolution of Terrorism as Legal Concept in International Law and its Influence on Definitions in Domestic Legislation*, 29 B.C. INT'L & COMP. L. REV. 23, 53 (2006).

> (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

This definition consists of several elements: first and foremost, the causation of physical harm to a victim who is a civilian or other person not taking an active part in the hostilities in a situation of armed conflict. From this stems the conclusion that an act which does not involve physical harm could not be considered an act of terrorism.[7] The physical harm is usually aimed at targets which possess a symbolic value and/or potential to cause great damage. For instance, suicide bombers on buses probably do not pick their targets because of any symbolic value that is attributed to them, but pick them due to their accessibility and the amount of potential damage they may achieve. Events like 9/11 or the bombing of the Israeli embassy in Buenos-Aires, on the other hand, clearly carry a symbolic statement in addition to its potential to cause massive destruction.[8]

The second element is the attacker's intention. Terrorism does not happen by accident. Terrorists seek to influence three main groups – the immediate victims of the terrorist act, the rest of the public in whom the terrorist act has engendered a sense of fear and the policymakers on a national or international level.

A part of terrorists' success derives from the fact that none of the attackers' potential victims feels protected; nobody knows when terrorism will strike next. This brings about the continuous state of terror (from the Latin word *"terrere"* – to frighten), creating an aftermath of fear long after the event itself took place. By hurting a group of random victims[9], terrorists hope to create widespread intimidation or fear, with which they wish to change human policy or course of action.[10] Generally speaking, the principal targets of a terrorist episode are not the victims who are killed or maimed in the attack, but rather the governments, publics, or constituents among whom the terrorists hope to produce a reaction.[11]

Despite its comprehensive quality, the Financing Convention does not

---

[7] Daniel M. Schwartz, *Environmental Terrorism: Analyzing the Concept*, 35(4) J. PEACE RES. 483, 485-486 (1998).

[8] *Id*.

[9] Gilbert Guilaume, *Terrorism and International Law*, 53 INT'L & COMP. L.Q. 537, 541(2004).

[10] Schwartz, *supra* note 7, at 485-486.

[11] Cronin, *supra* note 2, at 32.

address the identity of the terrorists. It defines only the activity and not the actor. Thus, the definition may include individuals, groups and even state entities. Nonetheless, for the purposes of this essay I will refer to "Terrorism" as it is defined in the Financing Convention. It is worth noting that most scholars have identified acts of terrorism as consisting of the same elements enumerated in the Financing Convention – causing physical harm with the intent to create a sense of fear and influence governmental processes.[12]

The UN approach toward combating Terrorism consisted of two main courses of action – condemning the general phenomena and suppressing specific manifestations of it.[13] The current international regime against terrorism consists of thirteen international conventions and protocols as well as seven regional conventions.[14] The international conventions deposited with the UN secretary cover issues like civil aviation, maritime, protection of diplomatic agents, hostage situations, and more. Member states are currently negotiating a fourteenth international treaty intended to be a comprehensive convention on

[12] Walter Enders, Adolfo Sachsida & Todd Sandler, *The Impact of Transnational Terrorism on U.S. Foreign Direct Investment*, 59(4) POL. RES. Q. 517, 518 (2006). *See also* Guilaume, *supra* note 9, at 540.

[13] Shaw, *supra* note 3, at 1049.

[14] The international conventions are: Convention on Offenses and Certain Other Acts Committed on Board Aircraft, Sep. 14, 1963, 704 U.N.T.S. 219; Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 860 U.N.T.S. 105; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Sep. 23, 1971, 974 U.N.T.S. 178; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, Dec. 14, 1973, 1035 U.N.T.S. 167; International Convention against the Taking of Hostages, Dec. 17, 1979, 1316 U.N.T.S. 205; Convention on the Physical Protection of Nuclear Material, Mar. 3, 1980, 1456 U.N.T.S. 246; Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Feb. 24, 1988, 1652 U.N.T.S. 499; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Mar. 10, 1988, 1678 U.N.T.S. 221; Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, 1678 U.N.T.S. 304; Convention on the Marking of Plastic Explosives for the Purpose of Detection, Mar. 1, 1991, 30 I.L.M. 721; International Convention for the Suppression of Terrorist Bombings, Dec. 15, 1997, 2149 U.N.T.S. 256; Financing Convention, *supra* note 4; International Convention for the Suppression of Acts of Nuclear Terrorism, Apr. 13, 2005, UN Doc. A/RES/59/290.

The regional conventions are: Arab Convention on the Suppression of Terrorism, Apr. 22, 1998; Convention of the Organization of the Islamic Conference on Combating International Terrorism, Jul. 1, 1999; European Convention on the Suppression of Terrorism, Jan. 27, 1977; OAS Convention to Prevent and Punish Acts of Terrorism Taking the Form of Crimes against Persons and Related Extortion that are of International Significance, Feb. 2, 1971; OAU Convention on the Prevention and Combating of Terrorism, Jul. 14, 1999; SAARC Regional Convention on Suppression of Terrorism, Nov. 4, 1987; Treaty on Cooperation among States Members of the Commonwealth of Independent States in Combating Terrorism, Jun. 4, 1999.

international terrorism, as will be elaborated *infra*.[15]

UN efforts to fight terrorism are also carried out through the Security Council. Prior to 9/11, the Security Council efforts to combat international terrorism took the form of sanctions against states considered to have links to certain acts of terrorism, such as Libya and Sudan. In 1998, after the terrorist bombings in Kenya and Tanzania the Security Council adopted Resolution 1189.[16] This resolution included a short statement on condemning terrorism and called upon states and international institutions to cooperate on the matter. It did not, however, impose any sanctions. In resolution 1269 of October 1999, the Security Council began advancing towards a more operative course of action, and requested the Secretary-General of the UN "to pay special attention to the need to prevent and fight the threat to international peace and security as a result of terrorist activities."[17]

After 9/11 the Security Council began addressing the issue of international terrorism more vigorously as was expressed in Security Council Resolution 1373.[18] Adopted under Chapter VII of the UN Charter, Resolution 1373 declares international terrorism "a threat to international peace and security." It imposes binding obligations on all UN member states such as the prevention and the suppression of the financing of terrorist acts, the criminalization of terrorism-related activities and providing assistance to carry out those acts, the denial of funding and safe haven to terrorists and the exchange of information to prevent the commission of terrorist acts. The resolution also establishes a "Counter Terrorism Committee" (CTC) to monitor implementation of the resolution, with all states being required to report back to the CTC regarding steps taken to execute Resolution 1373.[19]

In December 2004, the UN High-Level Panel on Threats, Challenges and Change published a report calling for the creation of a comprehensive global counter-terrorism strategy, encompassing the various counter-terrorism activities under the leading role of the UN. Two years later, on September 2006, the General Assembly created the UN Global Counter Terrorism Strategy.[20] The Annex to this Resolution established a "Plan of Action", specifying various measures to be taken by the Member States domestically and

---

[15] General Assembly, *Report of the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996, Seventh Session*, U.N. Doc. A/58/37, Supplement no. 37 (31 March – 2 April 2003).

[16] S.C. Res. 1189, U.N. Doc. S/RES/1189 (Aug. 13, 1998).

[17] S.C. Res. 1269, U.N. Doc. S/RES/1269 (Oct. 19, 1999), ¶ 5.

[18] S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sep. 28, 2001).

[19] *Id*, at ¶ 6. *See also*Eric Rosand, *Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism*, 97(2) AM. J. INT'L L. 333-341 (2003).

[20] G.A. Res. 60/288 U.N. Doc. A/RES/60/288 (Sep. 8, 2006).

internationally. These measures were designed to enhance both international cooperation to prevent and combat terrorism and the UN role within this cooperation, as well as strengthening the individual state's commitment and ability to eliminate terrorism in its territory and create "a culture of peace." The effectiveness of this Strategy has yet to be determined.

II. CYBERTERRORISM: THE NEW THREAT

Over a decade ago, in 1998, Ehud Tenenbaum, an 18-year-old Israeli hacker known as the "Analyzer," penetrated the computer systems of the Pentagon, NASA, the Massachusetts Institute of Technology, the Naval Undersea Warfare Center and other highly protected computer systems in the U.S. A U.S. Defense Department official called it "the most organized and systematic attack the Pentagon has seen to date."[21] Tenenbaum's hacking operation was even given a code name, the "Solar Sunrise," by the F.B.I. In 2001, a 16-year-old from Canada, called "Mafia Boy" also managed to pass the information security systems of some of the most sensitive computer infrastructures in the U.S.

During the past ten years information security systems grew more sophisticated, but so did hackers. This section asks the question – "What if?" What if Ehud Tenebaum and "Mafia Boy" had been members of a terror organization? What if they had been able to penetrate highly sensitive information in the Pentagon? What if they had covered their tracks better?

Terrorist groups have been using the Internet for various purposes, such as communicating, propagandizing, recruiting and collecting intelligence.[22] The network of computer-mediated communication is ideal for terrorists as communicators: it is decentralized, it is more difficult to subject it to control or restriction and it allows access to anyone who wishes to use it.[23] However, the cyber-world can also be used in a different way, not only as an indirect tool for executing an attack, but also as a direct weapon.

One way to use the weapon of cyberspace is through cyberattacks on websites. For instance, such attacks have taken place in the India-Pakistan dispute over Kashmir, in the context of the Israeli-Palestinian conflict and

[21] *Master hacker 'Analyzer' held in Israel*, Mar. 18, 1998, *available at* http://www.cnn.com/TECH/computing/9803/18/analyzer/index.html.

[22] Gabriel Weimann, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGES (2006). *See also*: Benjamin R. Davis, *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance*, 15 COMMLAW CONSPECTUS 119-186 (2006).

[23] *Id.* at 25.

against NATO websites during the crises in Kosovo in the early 1990's.[24] These attacks still do not constitute "terrorism" in the sense that they do not cause physical harm and do not intend to influence the government, as required by the definition of terrorism in the Financing Convention.

The other way of using cyberspace as a weapon is the case of cyberterrorism. Cyberterrorism is the use of computer networks in order to harm human life or to sabotage critical national infrastructure in a way that may cause harm to human life.[25] Joel Trachtman distinguishes between different types of networks that may be subjected to cyberterrorist attacks: military and civilian defense networks; other governmental networks (police, fire); privately or publicly owned networks used to control public utilities and other systems for providing infrastructural services (electricity, water); and public networks used by individual consumers and businesses for communication, education etc . . . [26]

Cyberterrorism may be disrupting bank data, penetrating rail company computers, blocking computer communication at an international airport, deleting the voter register 24 hours before an election, and many more. All these systems are service providers, which means they are linked to the Internet in one way or another and therefore are under the risk of invasion. Today, Western societies are dependent in almost every aspect of life upon computer communication. Computer systems control nearly everything required for our daily routines and our emergency plans.

But is cyberterrorism similar in its characteristics to other forms of terrorism mentioned earlier? Surely there must be some difference between hijacking an airplane with a gun and hijacking it by taking control over the airplane's computer system. Establishing the legal nature of cyberterrorism is crucial in combating it through international legal instruments, which, as was demonstrated above, are central to the international community's fight against terrorism.

As stated above, terrorism exhibits the elements of physical harm and

---

[24] Janet J. Prichard & Laurie E. MacDonald, *Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks*, 3 J. INFO. TECH. EDU. 279, 281 (2004).

[25] This is according to Shlomo Harnoy, Founder, senior VP & Professional manager at SDEMA Group, and Yossi Or, VP Information Security at SDEMA Group. The SDEMA Group is an integrated, homeland security solutions partnership specializing in risk mitigation. SDEMA also offers information security service including market forward protection against cyber terrorism. This definition is also accepted in academic literature, *see* Weimann, *supra* note 22, at 148; Dorothy E. Denning, "Cyberterrorism": Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

[26] Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, and International Organization*, Jul. 20, 2004, *available at* http://ssrn.com/abstract=566361.

intention to cause a sense of fear and to influence the decision making process. The cause of physical harm can be attained through disruption of computer systems, such as disabling traffic light systems, hospital computers, electric companies' computer etc . . . These acts bring about a sense of fear and uncertainty among the victim population, which in turn leads to pressuring the government to "do something" about it. Thus, you do not need to go through the trouble of getting a gun or a knife onboard an aircraft in order to become a terrorist. You can get the same results sitting in front of a computer screen.

In addition, most of the potential infrastructure targets of cyberterrorism, like those stated above, are protected by some sort of information security and anti-virus programs. Penetrating these programs takes time and knowledge, and it happens solely if the hacker intends for it to happen. Of course not every Ehud Tenenbaum is a terrorist just because he intended to break into classified computer networks. As the abovementioned definition requires, the intention element also means there was intention to influence a government course of action.

Regardless, cyberterrorism has several unique characteristics distinguishing it from other forms of Terrorism.[27] We defined Terrorism as being aimed at a certain target that has great potential damage in terms of human life. The identity of the humans itself did not matter. Cyberterrorism, on the other hand, can hurt a very specific group of people – the population of modern western countries.

As stated above, cyberterrorism hurts computerized infrastructure, on which advanced societies have come to depend. Thus, different societies are vulnerable to cyberterrorism in different degrees in accordance with their level of dependence on technology and computer networks. The more dependent a state is on electronic communications and information processing networks, the more vulnerable to cyberterrorism it will be.[28] As Richard Clarke put it already in 1999 – "If you are connected you are vulnerable."[29]

One might say that the level of technology advancement also results in better defense systems, which enable states to protect themselves from these kinds of attacks. This is correct, yet while assessing the volume of the risk, it remains clear that the U.S. is more exposed to cyberterrorism than Rwanda. This, in turn, will force the cyberterrorists trying to attack the U.S. to become more sophisticated themselves. Still, these cat and mouse games between the

[27] Susan W. Brenner & Marc D. Goodman, *In defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, J.L. TECH. & POL'Y 1, 12 (2002).

[28] Weimann, *supra* note 22, at 148; Trachtman, *supra* note 26, at 5.

[29] Richard Clarke, *Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks*, 12 DEPAUL BUS. L.J. 33, 37 (1999-2000).

cyberterrorists and the information security experts are most likely to occur in the U.S. and not in Rwanda because the U.S. has more at stake – it is more dependent on its information security to hold on against a cyberterrorism attack because it is more dependent on computerized infrastructure.

Another distinctive feature of cyberterrorism is its relatively low costs. A terrorist attack in the physical world requires recruiting an executor, equipping him with weapons or explosives and making sure he will pass all security checks on his way to the designated location. Cyberterrorism on the other hand, will most likely save the terrorist these costs and obstacles. Committing a cyber-attack, assuming you know how, does not involve purchasing weapons or actually being present at the attack's location. All a cyberterrorist needs is a good computer and hacking skills that exceed his opponent's. In today's world, anyone has the potential to acquire the required technical skills, as a crash-course "Hacking 101" can be easily be found on the Internet itself.

Despite all the gloomy predictions of a cyberterrorism doomsday, no single instance of real cyberterrorism has yet been recorded. This fact leads people to think that the prophecies on cyberterrorism are exaggerated.[30] However, there are several arguments that need to be considered. Theoretically speaking, just because an event has not yet happened, does not affect the possibility of it happening in the future. Similarly, the superpowers in the international system have been preparing for the scenario of a nuclear war even though it is also based on an event that, fortunately, has not occurred. In addition, like physical terror cells that hold "sleeping agents" at their enemy's territory ready to be active on a phone call, so too can computer viruses be programmed to be active as of a certain date in the future, until which time no one will know of their existence.

Shlomo Harnoy and Yossi Or, both experts in the field of counter-terrorism, have pointed out that a possible reason as to why there have been no cyber-attacks could simply be that terrorist organizations have not yet acquired the technological ability, which is the core factor in cyberterrorism.[31] Other reasons are difficult to discern. At least in theory this is a highly effective weapon for terrorists. Assuming that the reason there has, of yet, been no cyberterrorism event is indeed the technological gap between the potential targets and potential terrorist, this calls for immediate action. Technological gaps can be closed, rapidly. Since the most critical infrastructures in Western societies are networked through computers, the potential threat of

[30] Weimann, *supra* note 22, at 149.

[31] *See also* Brenner & Goodman, *supra* note 27, at 44-52.

cyberterrorism is, at least in theory, alarming.[32]

Governments in Western countries have been taking cyberterrorism threats very seriously for at least a decade. For instance, the U.S. authorities conducted the first experiment of its kind, designed to check the level of readiness of U.S. computer systems for the next attack. This operation was held in 2002 and was given the symbolic name "Digital Pearl Harbor." The results were startling. The "Red Team," which was supposed to try to hack into computer systems and disrupt their functioning, succeeded in nearly all cases.[33] After this experiment the U.S. government began a campaign of improving readiness for cyberterrorism, both on the technical and legislative level.[34]

In Israel, Government Decision B-84 from 2002 defined critical data systems that will undergo a security upgrade to adjust their information security systems to a scenario of cyberterrorism. In Europe, governments have acted not only on a singular basis, such as the establishing of the National Technical Assistance Center in the United Kingdom,[35] but also in the framework of the European Union. In 2005 the European Council adopted the European Program for Critical Infrastructure Protection (EPCIP) as part of its overall fight against terrorism. The EPCIP focuses mainly on strengthening the computer security systems, in order to enhance the preparedness for terrorist attacks involving critical infrastructure.

Currently there is no international legal instrument which deals specifically with cyberterrorism. Since the threat seems not to be far fetched, it is prudent thinking to try and see what the legal international community has in store for the "Day After." Accordingly, the following chapters will examine the question of whether the existing international regime on terror, as previously described, is adequate for an event of cyberterrorism. If it is – the international community has sufficient legal instruments in case the next Ehud Tenenbuam is a terrorist. If it is not – some alternatives must be considered.

---

[32] Weimann, *supra* note 22, at 148; *see* Brenner & Goodman, *supra* note 27.

[33] Eric Purchase & Franch Caldwell, *Digital Pearl Harbor: a Case Study in Industry Vulnerability to cyber Attacks*, in: Sumit Ghosh, Manu Malek & Edward A. Stohr (eds.), GUARDING YOUR BUSINESS – A MANAGEMENT APPROACH TO SECUIRTY (2004).

[34] Tara Mythri Raghavan, *In fear of Cyberterrorism: An Analysis of the Congressional response*, J.L. TECH. & POL'Y 297-312 (2003).

[35] Clive Walker, *Cyberterrorism: Legal Principle and Law in the United Kingdom*, 110(3) PENN ST. L. REV. 625-665 (2006).

III. INTERNATIONAL COUNTER TERRORISM CONVENTIONS AND THEIR APPLICABILITY TO CYBERTERRORISM: TWO CASE-STUDIES

The previous section presented cyberterrorism as the next phase in the evolution of terrorism and as one of the significant threats to future international peace and security. While information security experts are assigned with the task of maintaining the technological gap in favor of the governments over the cyberterrorists, it is in the hands of international law experts to make sure that the international community is prepared for the "day after" the first cyberterrorism attack.

The legal analysis of the international response to cyberterrorism begins with an examination of the existing legal framework. In order to determine the applicability of any of those conventions to cyberterrorism, the first step is to make sure that the offenses defined in them are not limited to execution by physical means. As explained earlier, the current conventions were originally designed to respond to specific manifestations of terrorism, and hence they create specific offenses to suit each scenario, such as aircraft hijackings or hostage situations. Since most of these conventions were drafted when cyberterrorism was considered to be, at most, science fiction, it is not at all certain that they apply to a cyber attack.[36]

The next sections provide the legal background to treaty interpretation and examine three of the thirteen counter-terror conventions to see whether they apply to cyberterrorism or not. The selection of those three particular treaties is by no means exhaustive regarding the question of applicability, and further examination of all counter terror conventions is needed. However, due to the limits of the current research I have chosen to focus on leading conventions from different fields of terror, namely: terrorism aimed at aircrafts and terrorist bombings.

A. Interpretation of International Conventions

International law, much like domestic legal systems, suffers from an inherent deficiency – it creates legal regimes to correspond with a given reality but which might not be suitable to address changes in that reality. The instrument developed to cope with this problem is the notion that treaties, like

[36] This can be said with respect to any new method of terrorism that may evolve, for further reading on the criticism of the counter-terrorism conventions and their failure to address new methods of terrorism, *see* Jennifer Trahan, *Terrorism Conventions: Existing Gaps and Different Approaches*, 8 NEW ENG. INT'L & COMP. L. ANN. 215, 221-222 (2002).

domestic constitutions, are "living documents." This allows deviating from the strict literal meaning of the text as long as it fulfills the rationale of the text. Hence, a text that was written five years ago or one-hundred-years ago can maintain its relevance. In contrast, there is a point of view which holds that a legal document should be read in the context in which it was written. As will be seen, the controversy between these two theories of interpretation is reflected in the attempt to adjust existing conventions to a threat that did not concretize at the time of drafting.

The issue of interpretation of international law was codified in 1969 in the Vienna Convention on the Law of Treaties[37] (The Vienna Convention), also know as the "Treaty on Treaties."[38] Articles 31-33 set forth the interpretive norms and rules for all treaties concluded between states.[39] The Vienna Convention, including Articles 31-32, is widely considered to reflect customary international law by scholars[40] as well as by the International Court of Justice.[41]

Most scholars agree that Article 31 puts a strong emphasis on a textual approach to treaty interpretation.[42] The preference of the textual approach, however, is not absolute. The recourse to contextual interpretation exists at the end of Article 31(1). In addition, Article 31 allows relying upon sources other than the text of the treaty, but only to the extent that the parties agreed to

[37] Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331.

[38] Richard D. Kearney & Robert e. Dalton, *The Treaty on Treaties*, 64 AM. J. INT'L L. 495-562 (1970).

[39] A separate convention governs the interpretation of agreements between states and international organizations and agreements between international organizations, see: Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations, Mar. 21, 1986, 25 I.L.M. 543. Since Article 33 deals with preference of translation issues, it does not concern the following treaty analysis and it will not be discussed.

[40] Shaw, *supra* note 3, at 839; Anthony Clark Arend, *Who's Afraid of the Geneva Convention? Treaty Interpretation in the Wake of Hamdan v. Rumsfeld*, 22 AM. U. INT'L L. REV. 709, 722 (2007); Jared Wessel, *Relational Contract Theory and Treaty Interpretation: End-Game Treaties v. Dynamic Obligations*, 60 N.Y.U. ANN. SUR. AM. L. 149, 162 (2004); Evan Criddle, *The Vienna Convention on the Law of Treaties in U.S. Treaty Interpretation*, 44 VA. J. INT'L L. 431, 438 (2004); P. Brazil, *Some Reflections on the Vienna Convention on the Law of Treaties*, 6 FED. L. REV. 223, 235 (1974-1975).

[41] *See e.g.* Territorial Dispute (Libya v. Chad), 199 I.C.J. 16; Legal Consequences for States of the Continued Presence of South Africa in Namibia (S. W. Afr.), 1971 I.C.J. 16; Appeal Relating to the Jurisdiction of the ICAO Council (India *v.* Pak.), 1972 I.C.J. 46; Nuc lear Tests (Austl. *v.* Fr.), 1974 I.C.J. 253. *See also* adherence to the Vienna Convention by the Dispute Settlement Body of the World Trade Organization: Panel Report, *Colombia — Indicative Prices and Restrictions on Ports of Entry*, WT/DS366 (Apr. 27, 2009) ¶ 7.81.

[42] Arend, *supra* note 40, at 723; Michael P. Van Alstine, *Dynamic Treaty Interpretation*, 146(3) U. PA. L. REV. 687, 744 (1998); Wessel, *supra* note 40, at 163; Criddle, *supra* note 40, at 438; Brazil, *supra* note 40, at 236.

consider those sources as providing authoritative interpretive information.[43] Due to rapid technological changes, the text of an agreement might become obsolete. This creates a need to expand the treaty, either implicitly or explicitly, so as to cover new circumstances.[44] It should be noted that another possible way of addressing changes in circumstances is to conclude a new treaty. While the latter option is examined further ahead in Part III, the following examination centers on the use of interpretation as a means of adjusting legal texts to changes in the legal reality.

Article 32 allows the interpreter to use the negotiating history (*travaux préparatories*) in order to confirm the analysis reached under Article 31, and seems to give only secondary place to the exploration of the preparatory work.[45] On the other hand, Article 32 does not specify the extent of ambiguity or obscurity that must persist after completing the Article 31 analysis in order to trigger Article 32(a), thus, it could be argued that even reasonable doubt may justify recourse to Article 32.[46]

B. Case-Study #1: The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1971

A State Airline company is a national symbol. Though nowadays the number of privately owned airline companies is larger than in the past, these airline companies, as well as the state owned ones, are still subject to governmental oversight and regulation on the national as well as the international level. Their existence, routes, and most of their commercial activities are a product of governmental cooperation.[47] Commercial aviation disasters, intentional or accidental, are uniquely treated by the public and news media as singular events[48] An airplane contains the two features terrorists seek: it has a symbolic nature and an enormous damage potential. Furthermore, aviation disasters affect world order and economic relations between states,[49] as

[43] Arend, *supra* note 40, at 724.

[44] Wessel, *supra* note 40, at 177.

[45] Arend, *supra* note 40, at 725. *See* Eberhard P. Deutsch, *Vienna Convention on the Law of Treaties*, 47 NOTRE DAME LAW. 297, 299 (1971).

[46] Criddle, *supra* note 40, at 440.

[47] Humphrey G. Dawson, *Civil Aviation, Hijacking and International Terrorism – An Historical and Legal Review*, 15 INT'L BUS. LAW 53, 57 (1987).

[48] Amon Haruta & Kirk Hallahan, *Airline Crisis Communication: A Japan-U.S. Comparative Study*, 13(1) ASAIN J. COMM. 122-150 (2004). *See also* William A. Crenshaw, *Civil Aviation: Target for Terrorism*, 498 ANNALS AM. ACAD. POL. & SOC. SCI. 60-69 (1988).

[49] Dawson, *supra* note 47, at 57.

aviation is a key factor in international trade.[50]

For these reasons and others, commercial aircrafts have been prominent targets of terrorist attacks.[51] Aviation terrorism manifests itself by means such as hijacking an aircraft, firing heat-seeking missiles at an aircraft, bombing an aircraft or airport lounges, gunning down passengers at airports, and more recently, turning aircrafts into guided missiles aimed at financial and governmental institutions.[52]

International law has dealt with aviation safety since the early years of the twentieth century. As soon as an airline route was established between Paris and London it was obvious that basic standards and principles in this new field were needed. In 1919, the Convention for the Regulation of Aerial Navigation[53] was signed in Paris, creating for the first time an international aviation organization, known as CINA. In 1944, after World War II presented new frontiers to military as well as civil aviation, fifty-two world nations met in Chicago, U.S., and drafted a new convention, the Convention on International Civil Aviation.[54] This Convention established the International Civil Aviation Organization (ICAO), a specialized agency that became a part of the United Nations, and replaced CINA.[55]

Though the Paris and Chicago conventions dealt extensively with flight safety regulation, they did not deal with aviation security. The first effort was made in 1963, at the Convention on Offenses and Certain Other Acts Committed on Board Aircraft, signed in Tokyo,[56] to assert formal international control over criminal acts such as hijackings.[57] Following the *aut dedere aut judicare* principle, the Tokyo Convention was designed to insure that when an offense[58] was committed on board an aircraft in flight, at least one state would

---

[50] Michael Milde, *The International Civil Aviation Organization: After 30 Years and Byond*, 1996 AUSTL. INT'L L.J. 61 (1996).

[51] Paul S. Dempsey, *Aviation Security: The Role of Law in the War Against Terrorism*, 41 COLUM. J. TRANSNAT'L L. 649, 651 (2003). *See also* Gerald F. Fitzgerald, *Aviation Terrorism and the International Civil Aviation Organization*, 25 CAN. Y.B. INT'L L. 219, 221 (1987).

[52] Dempsey, *supra* note 51, at 651.

[53] Convention Relating to the Regulation of Aerial Navigation, Oct. 13, 1919, 11 L.N.T.S. 173.

[54] Convention on International Civil Aviation, Dec. 7, 1944, 15 U.N.T.S. 295. (hereinafter: "Chicago Convention").

[55] For further reading on the ICAO see: Milde, *supra* note 50; Eugene Sochor, *ICAO and Armed Attacks against Civil Aviation*, 44 INT'L J. 134-170 (1988-1989); Fitzgerald, *supra* note 51.

[56] *See* Conventions, *supra* note 14.

[57] The first hijack attempt on a commercial aircraft occurred in 1931, but the first real wave of hijackings began around 1958 when individuals hijacked aircraft as a means to divert them from Cuba to the United States. *See* Dempsey, *supra* note 51, at 664; Dawson, *supra* note 47, at 59.

[58] Article 1(1)-(2) of the Tokyo Convention defines the offenses as follows:

"Article 1: (1) This Convention shall apply in respect of:

be able to exercise its jurisdiction over the offense and bring the offenders to justice.

Although the Tokyo Convention included a universal jurisdiction as a principle remedy, it in fact did not prove to be sufficient in confronting the increased number of acts of terrorism against aircrafts in the late 1960's. It was clear that there was a need for a broader definition of unlawful acts against aircrafts and a more definite statement as to the appropriate penalties than those offered by the Tokyo Convention.

The ICAO responded by adopting the Hague Convention of 1970.[59] The Hague Convention dealt specifically with acts of unlawful seizure of aircrafts,[60] and was considered a more efficient instrument than the Tokyo Convention. However, aviation terrorists began using methods that were not addressed by the Hague Convention, i.e. performing acts that did not constitute "seizing or exercising control over an aircraft." As quickly as 1971, only one year after the signing of the Hague Convention, there was already a need for further measures and for the creation of further criminal offenses.[61] Thus, in 1971, the ICAO drafted the Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (The Montreal Convention).

The Montreal Convention broadened the legal instruments available to combat aviation terrorism. It expanded the definition of "offense" beyond mere seizure as to include the general category of "interference with aircraft."[62] Though it was criticized for not addressing situations of state involvement in a

---

(a) offences against penal law;

(b) acts which, whether or not they are offences, may or do jeopardize the safety of aircraft or of persons or property therein or which jeopardize good order and discipline on board;

(2) Except as provided in Chapter III, this Convention shall apply in respect of offences committed or acts done by a person on board any aircraft registered in a Contracting State, while that aircraft is in flight or on the surface of the high seas or of any other area outside the territory of any State."

[59] *See* Conventions, *supra* note 14. See also: Dawson, *supra* note 47, at 60.

[60] Article 1 of the Hague Convention defines the offences as follows:

"Any person who on board an aircraft in flight:

(a) unlawfully, by force or threat thereof, or by any other form of intimidation, seizes, or exercises control of, that aircraft, or attempts to perform any such act, or

(b) is an accomplice of a person who performs or attempts to perform any such act

Commits and offence (hereinafter referred to as "the offence").

[61] Dawson, *supra* note 47, at 60.

[62] Dempsey, *supra* note 51, at 659. *See also* D.J. Musch, INTERNATIONAL TERRORISM AGREEMENTS AND COMMENTARY 41 (2004).

terrorist act, as was the case in the famous Lockerbie incident,[63] the Montreal Convention is still regarded as a primary instrument in dealing with aerial terrorism.

The Applicability of the Montreal Convention to a Cyberterrorism Attack

Article 1 of the Montreal Convention defines the offenses under the scope of the Convention. In the deliberation on the draft convention, some countries preferred the enumerative approach,[64] listing a limited number of specific offenses, while others supported a general definition.[65] The latter states argued that adopting a list of offenses would necessarily mean that future acts, unpredictable at the time of drafting, would be left out the scope of the Convention.[66] After much debate the enumerative approach was adopted, though the definition was drafted quite broadly, raising doubts regarding the actual difference between the two approaches. Article 1(1) states five alternative offenses being executed by the prime offender, and Article 1(2) criminalizes offenses of attempt and accomplice. Article 1(1) reads as follows:

> Any person commits an offence if he unlawfully and intentionally:
>
> (a) Performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft; or
>
> (b) Destroys an aircraft in service or causes damage to

[63] On December 1988, Pan Am flight 103 from London to New York was bombed over the town of Lockerbie, Scotland, killing 270 passengers, crew and local townsman. The U.S. and The U.K. accused Libya of being responsible for the attack, and brought the matter before the International Court of Justice. The ICJ was unable to establish that Libya had violated the Montreal Convention, since it did not address the issue of state-sponsored terrorism. *See* Case concerning questions of interpretation and application of the 1971 Montreal Convention arising from the aerial incident at Lockerbie (Libya v. U.K.) 1998 I.C.J. 9. For further reading see Jonathan A. Frank, *A return to Lockerbie and the Montreal Convention in the Wake of the September 11th Terrorist Attacks: Ramifications of Past Security Council and International Court of Justice Action*, 30(4) DENV. J. INT'L L. & POL'Y 532, 536 (2002).

[64] ICAO, *International Conference on Air Law: Minutes and Documents*, ICAO Doc. 9801, p. 21, Delegates of France and Japan (hereinafter: "ICAO Documents").

[65] *Id*., p.21, 27, Delegates of Canada and the People's Republic of the Congo.

[66] Abraham Abramovsky, *Multilateral Conventions for the Suppression of Unlawful Seizure and Interference with Aircraft, Part II: the Montreal Convention*, 14(2) COLUM. J. TRANSNAT'L L. 268, 280 (1975).

> such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight; or
>
> (c) Places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight; or
>
> (d) Destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight; or
>
> (e) Communicates information which he knows to be false, thereby endangering the safety of an aircraft in flight.

Considering the threat of cyberterrorism, which did not exist during the drafting of the Montreal Convention, it is time to re-evaluate whether the offenses listed in Article 1 are applicable to a cyberterrorism event, or whether the predictions of the states who voted for the general definition turned out to be accurate. Unlike other conventions, the Montreal Convention does not include a definitions clause that would assist in interpreting its provisions. Thus, the legal analysis of the text is based on the rules of interpretation set in the Vienna Convention on the Laws of Treaties,[67] and other interpretation guidelines, mainly including the protocols of the Montreal Conference in which the draft convention was approved[68] and additional related literature.

The starting point of the discussion is that all five items listed in Article 1 reflect the notion that the Convention meant to protect the safety of an aircraft in flight, rather than protection of human life.[69] Therefore, intentionally endangering the life of a passenger without endangering the safety of the aircraft is not an offense covered by the Convention. It can, on the other hand, be argued that the two elements can not in fact be separated, and that one could not endanger the safety of the aircraft without endangering the lives of the crew and passengers in that aircraft and that the lives of the crew and passengers could not be put at risk without jeopardizing the safety of the aircraft.[70]

It should also be noted that according to the text of Article 1, there is no requirement that the perpetrators or their accomplices be on board the

[67] Vienna Convention, *supra* note 37, § 31, 32.

[68] ICAO Documents, *supra* note 64.

[69] Abramovsky, *supra* note 66, at 281.

[70] ICAO Documents, Delegate of the United Kingdom, *supra* note 64, at 27.

aircraft. This is another feature of the Montreal Convention which makes it more advanced than the Hague Convention. Unlike the Hague Convention, the provisions of the Montreal Convention may apply whether the alleged offender was on board the aircraft or on the ground. This enhances the likelihood that the Montreal Convention would be suitable for dealing with cyberterrorism against an aircraft, since as noted in the previous chapter, one of the advantages of cyberterrorism is the ability to execute an attack from a distant location.

The Montreal Convention also deals with offenses committed on board an aircraft "in service," as opposed to an aircraft "in flight."[71] This extends the period of time to which the provisions of the Convention are applicable. At the deliberation on the adoption of the draft convention, most participating states hesitated to adopt the "in service" period. Those states believed that as long as an offender on board an aircraft is subject to both arrest and prosecution in the state where the aircraft is confined, there is no need for international intervention.[72] This point illustrates that the focus of the Convention seems to be on *ex post* punishment rather than *ex ante* prevention.

Based on these starting points, the following analysis examines whether the different items listed in Article 1(1) are applicable to cyberterrorism. It is important to note that the primary aspect of my analysis is a legal, rather than a technical one. Thus, I assume that all the activities that will be mentioned below are technologically possible. My main purpose is to examine the language of the text and its possible interpretations.

(a) Act of violence against a person on board an aircraft in flight that is likely to endanger the safety of the aircraft

Article 1(1)(a) is designed to prevent and punish acts of violence committed against persons on board an aircraft in flight. The term "Act of

[71] Article 2 of the Montreal Convention defines the two categories as follows:

> (a) An aircraft is considered to be in flight at any time from the moment when all its external doors are closed following embarkation until the moment when any such door is opened for disembarkation; in the case of forced landing, the flight shall be deemed to continue until the competent authorities take over the responsibility for the aircraft and for persons and property on board;
>
> (b) An aircraft is considered to be in service from the beginning of the preflight preparation of the aircraft by ground personnel or by the crew for a specific flight until twenty four hours after any landing; the period of service shall, in any event, extend for the entire period during which the aircraft is in flight as defined in paragraph (a) of this Article.

[72] Abramovsky, *supra* note 66, at 278.

Violence" is in fact wider than the phrase of the original draft convention.[73] The original draft provided that Article 1(1)(a) would apply in case an offender commits "an armed attack against the life of a person on board." Adopting the "Act of Violence" term does not restrict the provision's applicability to the use of certain weapons, nor does it restrict the offense to acts which jeopardize the life of the victim.[74]

With respect to the term "Person," it is clear that an attack on the pilot or the navigator of an aircraft in flight would endanger the safety of the aircraft. The less obvious cases regard the attack upon a flight attendant or a passenger. As mentioned above, the criteria for applying this provision in a specific case is not the gravity of the violent act, but rather its likelihood to affect the safety of the aircraft in flight. Hence, a murder of a passenger or a crew member other then the pilot or the navigator may not constitute the offense.[75] On the other hand, since the Article requires only "likelihood" to endanger the safety of the aircraft, it may be argued that an attack on a passenger could create panic and hysteria that are possible to endanger the safety of the aircraft in flight. Similarly, attacking a flight attendant could endanger the safety of an aircraft in flight since the flight attendants possess vital skills in cases of emergency.

Can an "act of violence" against a "person" on board an aircraft in flight be carried out through Cyberterrorism? The answer to this question depends on the meaning given to the term "violence." While there is extensive literature on the meaning of the term "violence" in general philosophical writings, I chose to adhere to the legal interpretations given to it. Violence is usually associated with a physical element, but the physical element can be established in two ways. In the first, as described in Black's Law Dictionary, the physical element regards the attacker. Violence, according to this view, is referred to as an unjustified use of force.[76] If we were to adopt this interpretation, than Cyberterrorism would probably be excluded from the scope of Article 1(1)(a), given that the cyberterrorist is not using any physical force.

According to the second possible interpretation, it can be argued that the physical element is attributed not to the perpetrator, but to the victim. Thus, violence is established whenever physical harm was caused to the victim of a certain act.[77] This view is reflected in the deliberation held at the ICAO Conference. Since cyberterrorism may result in physical damage to persons, for

---

[73] *Id*, at 284.

[74] *Id*. *See* C. S. Thomas & M. J. Kirby, *The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, 22(1) INT'L & COMP. L.Q. 163, 165 (1973).

[75] Abramovsky, *supra* note 66, at 285.

[76] BLACK'S LAW DICTIONARY 1570 (6th ed. 1990).

[77] ICAO Documents, *supra* note 64, at 139.

instance by a plane crash or damage to the aircraft's pressure system, cyberterrorism can very well constitute the offense described in Article 1(1)(a). Thus, it is possible that item (a) will apply to a cyberterrorism attack on an aircraft.

(b) Destroying an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight

Article 1(1)(b) penalizes acts of sabotage against the aircraft itself. The destruction or damage must occur while the aircraft is "in service," but the particular act which causes the destruction of the aircraft may be performed before the aircraft is "in service."[78] This further expands the period to which the Convention can be applied. In addition, since the provision does not require causing harm to a person, the offense may be constituted whether or not the aircraft is occupied.[79] This is not to be taken lightly, as it establishes the applicability of other provisions of the Convention to a case of mere property damage.

Item (b) contains two key elements. First, the action taken by the offender should be "destroying" or "causing damage" to an aircraft in service. Second, that action must result in disabling the aircraft from flying or enabling it to fly but endangering its safety in flight. Much like the term "violence" in item (a), it is likely that the "destruction" and "damage" referred to in item (b) were also intended to include physical destruction or damage. There have been cases in which simple maintenance errors, such as losing screws or cutting wires, have resulted in devastating crashes. These acts can be performed by a terrorist who has access to the aircraft. In order for cyberterrorists to cause such damage, they must take control over computerized systems in the aircraft and through them achieve the same damage as the cutting of a wire. Since this item focuses on the result of the act, rather than on the means achieving those results, the text of Article 1(1)(b) could encompass damage to an aircraft caused by cyberterrorism.

[78] Thomas & Kirby, *supra* note 74, at 165.

[79] Abramovsky, *supra* note 66, at. 286.

(c) Places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight

Article 1(1)(c) was originally intended to deal with situations in which explosives or other incendiary devices are placed on board an aircraft.[80] The phrase "Any Means Whatsoever" was originally put in the Article with the purpose to encompass acts such as the use of mails or the airline food storage to place incendiary devices on board an aircraft.[81] A proposal by the delegate of Egypt to replace the former term with the general term "anything" was rejected, and the protocols of the Montreal Conference reveal that "any means whatsoever" was perceived as covering all possibilities.[82] With respect to this notion, "any means whatsoever" can be interpreted as cyberterrorism.

Can a cyberterrorist place a device or substance on board an aircraft in service that would destroy it or endanger its safety in flight? The answer is probably yes. The computers on board an aircraft are in charge of almost every function in the aircraft, including the most critical ones like igniting the engines, controlling the landing gear. Hence, it is possible that a cyberterrorist would plant software that would disrupt the aircraft's computer system in one of the ways enumerated in the provision. Thus, it appears that the language of item (c) is applicable to cyberterrorism.

(d) Destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight

Article 1(1)(d) includes situations of intentionally committing an act of interference with the operation of aeronautical communications.[83] In compliance with Article 28 of the Chicago Convention, "Navigation Facilities" means airport control towers, and radio and meteorological services used in international flights.[84]

Like in item (b), it appears that "destroying" or "damaging" air navigation facilities could be executed through cyberterrorism. Moreover, "interfering with their operation" may also be carried out through cyberterrorism. According to Michael Oron, aircraft engineer and former El-Al

[80] Abramovsky, *supra* note 66, at 286; Thomas & Kirby, *supra* note 74, at 166.

[81] ICAO Documents, *supra note* 64, at 38.

[82] *Id*, at 108.

[83] Thomas & Kirby, *supra* note 74, at 166.

[84] Chicago Convention, *supra* note 54.

representative at Boeing, the navigation system on board an aircraft was designed to be a closed circuit and independent system. This means that the sensors on the body of the aircraft which measure temperature and altitude could almost never be exposed to foreign disruption.[85]

While this may be a relief to the worry of cyberterrorists attacking those sensors, there are other navigation facilities that are conditional upon communication between ground control computers and the computers on board the aircraft. It is also important to note that item (d) sets the threshold at only likelihood to endanger the safety of an aircraft in flight. Taking this into consideration, it is possible to think of a computer interference with the line of communication between the ground and the aircraft. This could be carried out in a way that would interfere with the operation of the navigation facilities thus endangering the safety of the flight or through interference with the ground facilities directing the aircraft to landing or take off. This scenario is closely related to the following item (e).

(e) Communicates information which he knows to be false, thereby endangering the safety of an aircraft in flight

Article 1(1)(e) covers situations in which a person who himself is not on board an aircraft exercises control over the craft. According to the observer of the International Federation of Airline Pilots Associations at the Montreal Conference, such acts may be used to divert the aircraft to an aerodrome located in an area in which no maps were on board.[86] The safety of an aircraft in flight could be seriously endangered by such acts. This item also covers bomb hoax situations. In this sense, the requirement of knowledge eliminates cases where the false information was given in good faith.[87]

Using the phrase "communicate" makes the offense in item (e) applicable to cyberterrorism. When originally drafted, the scenario associated with item (e) was that of a vocal transmission between the ground and the aircraft, but in today's high-technological world, the transmission could be between the computers on the ground directly to the computers on board the aircraft. According to Amir Cohen,[88] an expert on communication systems, the communication systems of aircrafts are shifting from voice-based-

[85] Interview with Michael Oron, aircraft engineer and former El-Al representative at Boeing.

[86] Chicago Convention, *supra* note 64, at 42.

[87] Abramovsky, *supra* note 66, at 286.

[88] Amir Cohen is the C.E.O. of SigNext Wireless Ltd., a leading company in the design and development of innovative wireless communication system based on space diversity multiple access technology.

communication to data-communication. This shift greatly contributes to flight safety and enables ground control to monitor the aircraft activities more accurately in real-time. Nevertheless, this wireless communication between the aircraft computer systems and the ground control creates vulnerabilities and exposes it to cyberterrorism, just like any other computer communication system.

In 1988 a Supplementary Protocol to the Montreal Convention (the Protocol) was adopted.[89] The Protocol expands the scope of the Montreal Convention by constituting two additional offenses:

> 1. Any person commits an offence if he unlawfully and intentionally, using any device, substance or weapon:
>
> (a) Performs an act of violence against a person at an airport serving international civil aviation which causes or is likely to cause serious injury or death; or
>
> (b) Destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport,
>
> If such an act endangers or is likely to endanger safety at that airport.

With respect to item (a), it seems that it is possible that it will apply to cyberterrorism.[90] In addition, item (b) could probably also apply to cyberterrorism. The terms "destroy" and "damage" were discussed at length previously, and so I will concentrate on the phrase "disrupting the services of the airport." It is conceivable that this term could also be executed through cyberterrorism. Any computer activity that interferes with the standard operation of the computer systems in the airport could comply with this requirement of the offense.

In conclusion, the Montreal Convention and the Supplementary Protocol constitute provisions relating to seven international offenses regarding the field of aviation security. If in the future cyberterrorists would attack aircrafts or airports, any of those seven offenses could be applicable.

[89] *See* Conventions, *supra* note 14.

[90] For the discussion on the interpretation of the term "Act of Violence" and its relation to Cyberterrorism *see id*.

Nevertheless, their application is dependent upon the interpretation of terms such as "violence" and "destroys," in a way that can be countered by good arguments claiming for the literal meaning of the text. Furthermore, while these offenses seem to cover a wide range of possible cyberterrorist attacks, the lack of a clear and general prohibition on using computerized infrastructures for executing terrorist acts leaves a gap for cyberterrorism attacks that could not be covered by the abovementioned offenses.

C. Case-Study #2: The Convention for the Suppression of Terrorist Bombings, 1997

On June 25, 1996, a terrorist truck bomb exploded outside the northern perimeter of a military compound housing American and Allied forces in Khobar Towers, Dhahran, Saudi Arabia. The attack resulted in nineteen fatalities and hundreds of wounded. The perpetrators escaped, and no group or individual claimed responsibility for the bombing.[91]

The method of using bombs in terrorist attacks became frequent long before the Dhahran attack. Some scholars have commented that this form of terrorism proved itself to be quite efficient in comparison to former methods.[92] All through the 1970's and the 1980's terrorist groups such as the Irish Republican Army and ETA used car-bombs to generate destruction. According to the Terrorism Research Center, since 1960 there have been over 4,000 bombing attacks throughout the world. These include small local bombs with little to no injuries, as well as large bomb attacks such as the one against the Israeli embassy in Buenos Aires in March 1992, or the Oklahoma City bombing against an American federal building office complex in April 1995.[93]

Nonetheless, unlike prior terrorist bombing attacks, the Dhahran bombing attack had an imperative impact on the international community's response to such terrorist bombings. After the attack, the U.S. military and intelligence community were heavily criticized for a lack of foresight that was considered an intelligence failure that could have been avoided.[94] Even more profound was the observation by U.S. officials that the attack was not an

[91] "Massive bomb rocks U.S. military complex", report by CNN, Jun. 26, 1996,*available at* http://www.cnn.com/WORLD/9606/25/saudi.explosion.

[92] Robert A. Pape, *The Strategic Logic of Suicide Terrorism*, 97(3) AM. POL. SCI. REV. 343-361 (2003).

[93] *See* http://www.terrorism.com.

[94] Douglas Jehl, *Fatal Lapses – A Special Report: How U.S. Missteps and Delay Opened Door to Saudi Blast*, N.Y. TIMES, Jul. 7, 1996.

isolated case, but rather it was a part of an escalating global jihad ideology.[95]

One month after the Dhahran bombing attack, on late July 1996, the Group of Seven Major Industrialized countries (also known as the "G7") and the Russian Federation, met in Paris. At that conference the ministries of justice accepted an American proposal to develop a new international instrument on terrorist bombings.[96] It is a common view that the Dhahran bombing was the trigger for this initiative.[97] Shortly after, the UN established an Ad Hoc working group of the Sixth Committee on the subject. The working group based its work primarily on a draft of the convention submitted by France on behalf of the G7.[98]

The Working Group drafted a Convention for the Suppression of Terrorist Bombings (the Bombing Convention). The draft was criticized by developing countries for lacking a clear definition of what "terrorist bombing" is, and was perceived as a tool of the developed countries to gain jurisdiction over political offenses outside their territories.[99] In spite of these protests, the Convention was adopted by the UN on 15 December 1997 and entered into force on 23 May 2001.

The Bombing Convention prohibits bombing of targets that are certain to cause a large number of civilian casualties.[100] The Convention broadened and strengthened international enforcement and cooperation in cases of international terrorism.[101] By requiring member states to outlaw different types of weapons detonations, such as chemical, biological and radiological, the Convention filled a serious gap in the international law regime.[102] The Convention was based on the structure of prior counter-terrorism conventions[103] and was used as the core text for drafting the Financing Convention, which was

---

[95] Toussef M. Ibrahim, *Saudi Rebel are Main Suspects in June Bombing of a U.S. Base*, N.Y. TIMES, Aug. 15, 1996.

[96] Declaration of the G7 Ministerial Conference on Terrorism, Paris, France, Jul. 30, 1996, ¶ 17.

[97] Samuel M. Witten, *Current Developments: The International Convention for the Suppression of Terrorist Bombings*, 92(4) AM. J. INT'L. L. 774-781 (1998).

[98] U.N. Ad Hoc Committee on Terrorist Bombing, *Press Release L/2825 1st Meeting, U.N. Ad Hoc Committee on Terrorist Bombing*, Feb. 24, 1997.

[99] General Assembly, *Report by the Sixth Committee: Summery record of the 30th meeting*, U.N. Doc. A/C.6/52/SR.30 (Dec. 4, 1977).

[100] Bombing Convention, *supra* note 14, § 1. *See also* Anne-Marie Slaughter & William Burke-White, *An International Constitutional Moment*, 43 HARV. INT'L L.J. 1, 10 (2002).

[101] Witten, *supra* note 97, at 781.

[102] Seth Brugger, *International Law, Terrorism, and Weapons of Mass Destruction: Finding and Filling the Gaps*, 57 RUTGERS L. REV. 803, 819 (2005).

[103] Christopher C. Joyer, *International Extradition and Global Terrorism: Bringing International Criminals to Justice*, 25 LOY. L.A. INT'L & COMP. L. REV. 493, 527 (2003).

adopted two years later.[104]

The Applicability of the Bombing Convention to a Cyberterrorism Attack[105]

Article 2 of the Bombing Convention defines the offenses under the scope of the Convention. The Article contains three categories of offenses – an offense committed by the main perpetrator, an attempt to perform the offense, and various forms of accomplices. The following paragraphs will evaluate whether the Bombing Convention could apply in case of Cyberterrorism.

Article 2(1) of the Bombing Convention reads as follows:

> Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility:
>
> (a) With the intent to cause death or serious bodily injury; or
>
> (b) With the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or is likely to result in major economic loss.

The offenses in Article 2(1) consist of several elements. Since cyberterrorism differs from "physical" terrorism only in terms of the act being performed, and not in the state of mind of the terrorist performing it, the two alternatives regarding the intention of the offender will not be analyzed. A cyberterrorist has the same intentions as a "normal" terrorist and thus there will be no legal difference in attributing intention to either one of them. The discussion below will examine the applicability of the acts described in the Article in a cyberterrorism scenario.

The offense requires that the perpetrator performs one of four physical

---

[104] Financing Convention, *supra* note 4; Report of the Ad Hoc Committee, *supra* note 15, ¶ 32.

[105] The following interpretation of the Bombing Convention is based on numerous sources. First and foremost, the definition clause set forth in Article 1 of the Convention. As will be elaborated ahead, Article 1 sheds light on some key expressions in the offenses definition. In addition, the interpretation also relied on reports and protocols of the Working Group which drafted the Convention as well as other relevant literature.

actions– delivers, places, discharges or detonates an explosive or other lethal device", against one of four locations – "place of public use, a State or government facility, public transportation system or an infrastructure facility." The application of Section 2(1) to a cyberterrorism attack depends first and foremost on the meaning given to the phrase "explosive or other lethal device."

According to the definition set forth in Article 1(3), "an explosive or other lethal device" stands for one of two possible interpretations. First, it could mean "*an explosive or incendiary weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage.*" A computerized infrastructure would probably fall short from complying with this interpretation. A computer could be used to trigger a bomb, but a computer in itself can not function as a bomb. The only way to cause an explosion associated with computer based infrastructure is to attach an external bomb to it, or to use the computers as the "red buttons" for triggering the detonators.

The second possible interpretation for the aforementioned definition was a later addition to the negotiation of the Working Group, which specifies various forms of materials that their release could endanger the population.[106] According to Article 1(3)(b), "an explosive or other lethal device" could be "*a weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage through the release, dissemination or impact of toxic chemicals, biological agents or toxins or similar substances or radiation or radioactive material."* As opposed to the former interpretation, this definition may very well fit the profile of cyberterrorism.

Computer infrastructures monitor and control the functioning of highly dangerous and sensitive places, among which are nuclear reactors, biological and medical labs and power plants. Computers are in charge of monitoring levels of temperature, moisture, radiation and other data that is crucial to the safety of these facilities. Hence, these computerized systems, these "devices", could be subject to cyberterrorism and their disruption could lead to "causing death, serious bodily injury or substantial material damage through the release, dissemination or impact of toxic chemicals, biological agents or toxins or similar substances or radiation or radioactive material." Though designed for the opposite purpose, such computer systems could be viewed as having the capability of causing a large scale disaster.

Having established that "an explosive or other lethal device" could mean computerized infrastructure, can a cyberterrorist "deliver, place, discharge or detonate" it? On the basis of the guidelines in Article 31 of the Vienna

[106] General Assembly, *Report of the Working Group to the Sixth Committee on: Measures to Eliminate International Terrorism*, U.N. Doc. A/C.6/52/L.3, at 36-37 (10 October 1997).

Convention for the Law of Treaties, the text should be interpreted in light of its purpose. Therefore, it can be argued that disrupting the operation of a computer system in a way that causes dangerous materials to be released is the equivalent of detonating a bomb, or discharging it. Since the computer system is located at the targeted site prior to the attack, the actions of "delivering" and "placing" appear to be irrelevant. This interpretation is acceptable because the purpose of the text is not compromised by addressing cyberterrorism, although it could be countered by arguments supporting the literal approach to treaty interpretation.

The third and last parameter that is noteworthy is the locations category. These represent places where terrorist attacks had typically occurred and where the public would be put at the greatest risk of harm due to such attacks.[107] According to Article 1 of the Convention, all four items refer to physical locations such as public facilities or governmental buildings—[108]all locations in which cyberterrorists can execute attacks through "discharging or detonating" an "explosive or other lethal device."

In conclusion, the Bombing Convention allows a relatively flexible interpretation of the offense set forth in Article 2. Each element of the offense can embody a wide range of meanings, which gives the Convention a maximum coverage. Due to this fact, an offender in the meaning of the Bombing Convention could also be a cyberterrorist who interferes with computer-based systems in a way that generates a release of dangerous substances in or against a public place.

---

[107] Witten, *supra* note 97, at 776.

[108] Bombing Convention, *supra* note 14, § 1:

> "place of public use" means those parts of any building, land, street, waterway or other location that are accessible or open to members of the public, whether continuously, periodically or occasionally, and encompasses any commercial, business, cultural, historical, educational, religious, governmental, entertainment, recreational or similar place that is so accessible or open to the public.
>
> " state or governmental facility" includes any permanent or temporary facility or conveyance that is used or occupied by representatives of a State, members of Government, the legislature or the judiciary or by officials or employees of a State or any other public authority or entity or by employees or officials of an intergovernmental organization in connection with their official duties.
>
> "Public transportation system" means all facilities, conveyances and instrumentalities, whether publicly or privately owned, transportation of persons or cargo."
>
> "Infrastructure Facility" means any publicly or privately owned facility providing or distributing services for the benefit of the public, such as water, sewage, energy, fuel or communications."

IV. THE FUTURE REGULATION OF COUNTER CYBERTERRORISM

The previous section analyzed the applicability of the two international counter-terrorism conventions to cyberterrorism. The conclusion of this examination was that the current counter-terror regime might apply to a cyberterror attack, but it is not obvious that it will. There is a fair chance that a legal tribunal will prefer a literal interpretation of the counter-terror conventions and in doing so may exclude cyberterrorism from their scope.

This section offers five additional legal regimes for combating cyberterrorism, outside the current conventional regime. These alternatives are the Draft International Comprehensive Convention on Terrorism; the Council of Europe Convention on Cybercrime; a particular convention for the suppression of cyberterrorism; international criminal law as codified in the statute of the International Criminal Court; and Security Council resolutions. As will be illustrated ahead, each one of the abovementioned instruments has its own advantages and deficiencies.

A. Draft International Comprehensive Convention on Terrorism

In 1996, India transmitted to the Secretary General of the UN for consideration by Member States a Draft International Convention on the Suppression of Terrorism (Draft Convention).[109] The Draft Convention proposed by India was revised several times, until the latest draft was published by the Ad-Hoc Committee in 2002.[110] In many respects, the Draft Convention is similar to prior conventions.[111] The improvements the Draft Convention introduces relate to the coverage of *all* acts of terrorism and to a greater extent of prevention and cooperation obligation.

The literature highlights the role of the Draft Convention in strengthening the international community's condemnation of terrorism.[112] It places states which sponsor terrorism on a defensive side and assist in the creation of an international customary denunciation of terrorism.[113] In addition, it would complement and guide the work of the Counter Terrorism Committee

[109] Letter dated 01/11/96 from the permanent representative of India to the United Nations addressed to the Secretary General, UN Doc. A/C.6/51/6 (Nov. 1, 1996).

[110] Report of the Ad Hoc Committee, *supra* note 15.

[111] Trahan, *supra* note 36, at 231; Asli U. Bali, *International Law and the Challenge of Terrorism*, 9 J. ISLAMIC L. & CULT. 1, 19 (2004).

[112] Report of the Ad Hoc Committee, *Supra* note 15, Annex I.A, ¶ 8.

[113] Matthew Lippman, *The New Terrorism and International Law*, 10 TULSA J. COMP. & INT'L L. 297, 358 (2003).

established by the Security Council.[114]

The Draft Convention's potential contribution to the international struggle against terrorism is hampered by two weaknesses, holding back any progress towards its adoption.[115] First and foremost, the Draft Convention includes only a limited definition of terrorism.[116] For the Draft Convention to truly provide a comprehensive basis to combat international terrorism, it must be applicable to all acts, methods and practices of terrorism wherever and by whoever committed.[117] The definitional problem is expressed in two core issues – the execution of terrorist acts during armed conflicts,[118] and state-sponsored harboring of terrorists and colluding in terrorist crimes.[119]

Despite these weaknesses, the Draft Convention is still considered to be a significant step towards unifying international cooperation against terrorism.[120] The applicability of the Draft Convention to Cyberterrorism is examined with regard to the offense defined in the Draft Convention. However, it should be noted that the preamble to the Draft Convention defines the scope of the Convention so as to address the general category of "*acts, methods and practices of terrorism,*"[121] thus providing a relatively low threshold enabling interpretation that includes cyberterrorism under the scope of the Draft Convention.

According to the Draft Convention, each state party undertakes to establish the offenses set forth in Article 2 as criminal offenses under its

---

[114] Report of the Ad Hoc Committee, *Supra* note 15, Annex I.A, ¶ 2.

[115] Supplementing to the two main weaknesses, concerns were also raised regarding the compatibility of the Draft Convention to the standards of human rights protection. This point requires a complex and in depth debate on the relationship between terrorism and human rights, and because it does not address directly the applicability of the definition in the Draft Convention to cyberterrorism, it overflows the scope of the current examination. *See* Bruce Broomhall, *State Actors in an International Definition of Terrorism from a Human Rights Perspectibe*, 36 CASE W. RES. J. INT'L L. 421, 421 (2004).

[116] Lippman, *supra* note 113, at 357; Gerhard Hafner, *Certain Issues of the work of the Sixth Committee at the Fifty-Sixth General Assembly*, 97 AM. J. INT'L L. 147, 156 (2003).

[117] Malvina Halberstam, *The Evolution of the United Nations Position on Terrorism: from Exempting National Liberation Movements to Criminalizing Terrorism Wherever and by Whomever Committed*, 41 COLUM. J. TRANSNAT'L L. 573, 584 (2003).

[118] Trahan, *supra* note 36, at 231; Broomhall, *supra* note 115, at 428.

[119] John P. Grant, *Beyond Montreal Convention*, 37 CASE W. RES. J. INT''L L. 453, 471 (2005); Broomhall, *supra* note 115, at 428.

[120] Lippman, *supra* note 113, at 357-358.

[121] Draft Convention, Report of the Ad-Hoc Committee established by General Assembly resolution 51/210 of December 1996, General Assembley Official Records, fifty-seven session, Supplement no. 37 UN Doc. A/57/37, preamble.

domestic law.[122] The Draft Convention also addresses issues of jurisdiction, cooperation between states, prosecution and enforcement measures and more. Article 2(1)(b) provides that:

> Any person commits an offence within the meaning of this Convention if that person, by any means, unlawfully and intentionally causes serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or the environment, when the purpose of the conduct, by it nature or context, is to intimidate a population, or to compel a Government or an International Organization to do or abstain from doing any act.

Article 1(3) defines "infrastructure facility" as:

> Any publicly or privately own facility providing or distributing services for the benefit of the public, such as water, sewerage, energy, fuel, banking, communications, telecommunications and information networks.

The reference in Article 2(1)(b) to "any means" combined with the definition of "infrastructure facility" as including "communications, telecommunications and information networks," enables the offense set forth in the Draft Convention to apply to cyberterrorism attacks. Its language is wide enough and clear enough to address cyberterrorism directly. The main advantage of this is that there is no need to rely on interpretation methods which could be argued against by those who represent a different school of legal thought.

Using computer-based communications networks qualifies as "any means," and harming computer-based infrastructure, or an "infrastructure facility" is written in plain English. This leaves little room to argue that cyberterrorism falls short of the Draft Convention's definition of the offense. Nonetheless, while the Draft Comprehensive Convention offers a definition which can encompass cyberterrorism directly, there are still major issues withholding any progress towards its adoption.

[122] *Id.*, Article 4.

B. Regulation through the Council of Europe Convention on Cybercrime

In 2001, the Council of Europe adopted the Convention on Cybercrime[123] (Cybercrime Convention). The Cybercrime Convention is the product of four years of work by experts from the Council of Europe, the United States, Canada, Japan and other countries, and it is open for signature for all countries. The Cybercrime Convention's main objective, as set out in the preamble, is to pursue a common and harmonized criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

Although the term "cybercrime" implies crime occurring on the Internet or via the internet, the scope of the Cybercrime Convention goes beyond such crimes and also includes crimes that occur through the use of a computer and crimes that involve computers in general.[124] For instance, the Cybercrime Convention has been supplemented by an additional protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offense.[125] Also in this respect, it is worth mentioning that although the substantive law provisions relate to offenses using information technology, the Cybercrime Convention uses technology-neutral language so that the substantive criminal law offenses may be applied to both current and future technologies involved.[126] This approach has many advantages, and it may prevent the emergence of legal gaps in the future like the one we are facing now concerning cyberterrorism.

The Cybercrime Convention requires states parties to criminalize offenses included therein in their domestic laws. However, the convention was criticized for not including any guidelines detailing the elements required for those offenses, leaving the matter to the discretion of the states parties, thus leading to the creation of a de facto fragmented legal framework instead of fulfilling the purpose of the Cybercrime Convention which was to unify the legal handling of the issue.[127] The Cybercrime Convention set forth provisions

---

[123] Council of Europe Convention on Cybercrime, Nov. 8, 2001, E.T.S. 185. (hereinafter "Convention on Cybercrime").

[124] Sara L. Marler, *The Convention on Cyber-Crime: Should the United States Ratify?* 37 NEW ENG. L. REV. 183, 185 (2002).

[125] Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Jan. 23, 2003, E.T.S. 189.

[126] Convention on Cybercrime, Explanatory Report. *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

[127] For instance, Article 4(2) allows Parties to enter a reservation concerning the offense set forth in paragraph (1), in that they may require that the conduct result in serious harm. The interpretation of what constitutes such serious harm is left to domestic legislation. *See also* Shannon L. Hopkins,

regarding criminal sanctions, jurisdiction, mutual legal assistance and more. Chapter II of the Convention deals with substantive as well as procedural legal issues. Section 1 of Chapter II defines nine offenses divided into four different categories.

All the offenses contained in the Cybercrime Convention must be committed "intentionally" for criminal liability to apply. Thus, a preliminary question should be raised as to whether the *mens rea* of the "cyber-criminal" is different than that of the "cyber-terrorist." As noted in Chapter 1,[128] a mere "intention" to commit an attack does not render that attack a terrorist attack. For a terrorist, as opposed to a criminal, it is required that the intention was to use the attack in order to influence policy makers. Therefore it is unclear whether the term "intentionally" in the sense of the Cybercrime Convention also covers that type of intention.

However, if it is assumed that the special intention associated with terrorists could be proved with regard to the term "intention" in the Cybercrime Convention, then most of the various offenses included in the Convention could apply to cyberterrorism. Cyberterrorism attacks could be carried out through illegal access to a computer system without right,[129] or through the interception of non-public electronic data transfer.[130] It is also conceivable that infliction of damage to the integrity and proper functioning or the use of stored computer data or computer programs will be part of a cyberterrorist attack.[131] Similarly, the rest of the offenses described in the Cybercrime Convention could also take place during a cyberterrorist attack, namely, the hindering of the functioning of a computer system,[132] misuse of devices,[133] computer-related forgery, and fraud.[134] Specific offenses regarding child pornography[135] and intellectual property rights[136] are less relevant to cyberterrorism activities.

To summarize, the Council of Europe Convention on Cybercrime contains some offenses which could be carried out through cyberterrorism. Nevertheless, the *mens rea* attributed to the perpetrator is merely "intention," and not the unique intention characterizing terrorism, aiming for consequences

---

Cybercrime Convention: A Positive Beginning to a Long Road Ahead, 2 J. HIGH TECH. L. 101, 113 (2003).

[128] *Id*.

[129] Convention on Cybercrime, *supra* note 123, E.T.S. 185 at § 2.

[130] *Id*, at § 3.

[131] *Id*, at § 4.

[132] *Id*, at § 5.

[133] *Id*, at § 6.

[134] *Id*, at § 7, 8.

[135] *Id*, at § 9.

[136] *Id*, at § 10.

at a policy level, beyond the immediate damage itself. Moreover, the Cybercrime Convention provides only limited coverage. By June 2009 only forty-six states singed the Convention, out of which only twenty-six ratified it. This fact demonstrates how the political will of countries also plays a vital part in determining the effectiveness of legal instruments. Even if the Cybercrime Convention contained a *mens rea* relevant to terrorism, the adherence or lack thereof by states would be the key factor in assessing its value.

C. Sectoral Convention for the Suppression of Cyberterrorism

Already in August 2000 experts from Stanford University published "A Proposal for an International Convention on Cyber Crime and Terrorism" (The Stanford Draft).[137] The Draft builds upon the Council of Europe Convention on Cybercrime, which was in its final drafting stages. The Stanford Draft proposes to criminalize several conducts, including, *inter alia*, using cyber-systems to execute offenses specified in certain other treaties[138] and targeting critical infrastructures.[139] The Stanford Draft also suggests establishing an international agency for information infrastructure protection, a forum for developing standards and practices concerning cyber security.[140]

As opposed to the Council of Europe Cybercrime Convention discussed above, the Stanford Draft specifically addresses the correspondence between terrorism and computer communications based infrastructure. It does not concern aspects of cyber acts which may constitute cyber-crimes but not cyberterror. In contrast to the Draft Comprehensive Convention, the Stanford Draft states clearly that it shall not apply to activities related to an ongoing armed conflict.[141]

Since the Stanford Draft was drafted no further steps were taken towards presenting it before the UN Sixth Committee, and the project did not develop into a more substantive legal work. Theoretically, the Stanford Draft could become the basis to create an international convention for the suppression of cyberterrorism. However, since it was drafted there have been two important advancements which may render such a cyberterrorism convention obsolete.

---

[137] Abraham D. Sofaer, Seymour E. Goodman et al., *A Proposal for an International Convention on Cyber Crime and Terrorism*, Hoover Institution, Stanford University (2000).

[138] Of the counter-terror conventions, Article 3 refers to the following: Tokyo Convention, *supra* note 14; Hague Convention, *supra* note 14; Montreal Convention, *supra* note 14; Hostage Convention, *supra* note 14; Terrorist Bombings Convention, *supra* note 14.

[139] Convention on Cybercrime, *supra* note 123, E.T.S. 185 at Art. 3.

[140] I*d*. at Art. 12.

[141] *Id*. at Art. 20.

First, while the Stanford Draft remained an academic project, the Council of Europe's Convention on Cybercrime came into force. The latter created a framework that treats many issues that were also raised in the Stanford Draft. This poses a critical question mark before the proponents of the Stanford Draft, as to whether there is a further need to treat numerous issues parallel in both instruments, or is the Cybercrime Convention enough.

Second, the drafting of the Comprehensive Convention is already underway, and, as seen earlier, its definition of offenses could encompass cyberterrorism. Thus, the resources that would be invested into concluding the cyberterrorism convention could be devoted into concluding the comprehensive convention, a generally more practical goal.

On the other hand, an independent counter-cyberterrorism convention could be a perfect tailor-made instrument to deal with cyberterrorism. A separate convention could furnish specific clauses that are designed to address the special features of cyberterrorism. It can establish designated mechanisms and mutual assistance procedures that are relevant to cyberterrorism, but may be excluded from the Comprehensive Convention due to its more general nature. Still, the core obstacle in the way of such a solution is the current lack of an updated draft to present before the Sixth Committee, or any other forum for that matter.

D. Terrorism as an International Crime

On July 1, 2002, the Rome Statute, establishing the International Criminal Court (ICC), entered into force.[142] Terrorism was excluded from the Rome Statute, presumably due to the following grounds: the offense of terrorism was not well defined; some acts of terrorism were not deemed to be sufficiently serious to warrant prosecution by the ICC,[143] and there was

---

[142] Rome Statute of the International Criminal Court, Jul. 17, 1998, 2187 U.N.T.S. 90. (hereinafter "Rome Statute"). For a thorough discussion on the International Criminal Court, see: Antonio Cassese, INTERNATIONAL CRIMINAL LAW (2008); William Schabas, AN INTRODUCTION TO THE INTERNATIONAL CRIMINAL COURT (2004).

[143] Article 1 of the Rome Statute set forth that:

> "An International Criminal Court ("the Court") is hereby established. It shall be a permanent institution and shall have the power to exercise its jurisdiction over persons for the most serious crimes of international concern, as referred to in this Statute, and shall be complementary to national criminal jurisdictions. The jurisdiction and functioning of the Court shall be governed by the provisions of this Statute" (emphasis added).

In addition, Article 5(1) of the Rome Statute set forth that *"The jurisdiction of the Court shall be limited to the most serious crimes of concern to the international community as a whole." See*

considerable concern that the inclusion of terrorist crimes in the Statute would politicize the Court.[144]

Some scholars believe that the reason terrorism was not included in the Rome Statute was the fact that it was already proscribed under existing conventional arrangements.[145] In my opinion, this last argument is not as strong as the former ones, since genocide was also addressed as early as 1948[146] and it was still reiterated in the Rome Statute. The inclusion of genocide in the statute of the ICC allowed the ICC to have jurisdiction over it, rather than leave it to application of universal jurisdiction by states. Similarly, entrusting the ICC with jurisdiction over terrorism in general and cyberterrorism in particular, would mean including it in the statute.

Whatever the reasons may be, the idea to address terrorism through the Rome Statute was not entirely rejected. A Review Conference, anticipated to be held in early 2010 in Uganda,[147] should consider the crime of terrorism "with a view to arriving at an acceptable definition and its inclusion in the list of crimes within the jurisdiction of the Court."[148] There are important benefits to be derived from the inclusion of the crime of terrorism in the Rome Statute.[149] It could, for instance, assist states in bringing terrorists to justice, while overcoming domestic weaknesses which prevent them from doing so in local courts; and send a strong political signal about the seriousness with which the international community views international terrorism.[150]

The current mandate of the ICC is to hold jurisdiction with respect to four types of international crimes:[151] genocide; crimes against humanity, war crimes; and the crime of aggression. With regard to the latter, Article 5(2) of the Rome Statute provides that the ICC will have jurisdiction over the crime of aggression once an agreed definition of that crime is adopted. Since no such definition has yet been adopted, the following discussion will only address the first three categories of international crimes.

Is it possible to include cyberterrorism under the aforementioned

---

Grant, *supra* note 119, at 465.

[144] Christian Much, *The International Criminal Court (ICC) and Terrorism as an International crime*, 14 MICH. ST. J. INT'L L. 121, 126 (2006).

[145] Grant, *supra* note 119, at 465.

[146] The Convention on the Prevention and Punishment of the Crime of Genocide, Dec. 9, 1948, 78 U.N.T.S. 277.

[147] ICC, *Resolution ICC-ASP/7/Res.2, Adopted at the 7th plenary meeting*, (Nov. 21, 2008).

[148] United Nations Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court, 15-17 July 1998, UN Doc. A/CONF.183/13 (Vol. I), p. 72.

[149] Much, *supra* note 143, at 134-136.

[150] *Id*, at 135.

[151] Rome Statute, *supra* note 141, § 5.

crimes? Where genocide is concerned, the answer will probably be that it does not include terrorism, and therefore could not include cyberterrorism as well. This category represents an international offense that has a long history and clear parameters.[152] As to war crimes, it is possible that a systematic and large scale cyber attack against civilian objects could comply with the definition of war crimes as set forth in the Rome Statute.[153] Although a degree of overlap does exist between humanitarian law and terrorism, the relation between them is not entirely clear. The discussion above regarding the disagreement about whether to include acts of terrorism committed during an armed conflict under the scope of the Draft Convention demonstrates that controversy. As long as it is not clear if acts of terrorism are treated differently in the context of armed conflicts, there is still a long way to go before there is an acceptance in considering terrorism as a war crime.

The idea that the definition of the term "crimes against humanity" contained in the Rome Statute could include terrorism is not new, though not widely accepted.[154] Article 7 of the Rome Statute sets forth a list of acts which, if committed knowingly as part of a widespread or systematic attack directed against any civilian population, are considered crimes against humanity. Cyberterrorism is not suitable to be included in the first ten out of eleven acts enumerated in the Article. Such acts include, *inter alia*, murder, enslavement, deportation, torture and persecution. Those acts, as well as the rest of the acts listed, cannot be carried out through cyberterrorism. Harming communications infrastructure is not on the list. Even sub-article (k), which leaves room for future developments in the words of "other inhumane act" sets a high threshold for such inhumane acts to constitute crimes against humanity. It clearly states that the inhumane acts should be "of a similar character." Since cyberterrorism is by its nature different then the aforementioned acts, it will be difficult, if not impossible, to argue that it can be included under sub-Article (k).

To conclude, international criminal law is not helpful as long as there is no clear definition of terrorism as an international crime in the Rome Statute. As seen earlier, terrorism could not be addressed within the current international crimes. It is currently in the hands of the Review Conference to determine whether there will be a change in this respect, or whether terrorism will remain excluded from the Rome Statute.

---

[152] Grant, *supra* note 119, at 465.

[153] Rome Statute, *supra note* 141, § 8, in particular section (2)(b)(ii).

[154] Much, *supra* note 143, at 127-129.

E. Security Council Resolution on the Suppression of Cyberterrorism

The power of the Security Council to adopt legally-binding decisions, vested in it by Article 25 of the UN Charter,[155] is considered a strong and effective implementation tool which has a global application to all members of the UN.[156] In countries where international law is absorbed directly into the domestic legal system (i.e. a monastic system as opposed to a dualistic system), Security Council Resolutions are given the status of binding domestic legislation. A clear example of that is Resolution 1373,[157] which demonstrates the authority of the Security Council to take various obligations from the existing counter-terrorism conventions and apply them to all UN member states, regardless of whether they signed those conventions or not.[158]

When considering turning to the Security Council as an avenue to combat cyberterrorism, the issue of legitimacy should also be taken into account. On the one hand, it is an exclusive club of fifteen members that are not accountable to other UN organs.[159] Any one of the permanent five members ("P-5") has the ability to veto any resolution with which it does not agree without needing to provide an explanation, which enhances the political character of the Council.[160] On the other hand, it can react promptly to urgent global threats, especially in cases where international law does not provide an answer.[161] It might even be said that in addressing terrorism the traditional law making approach falls short from delivering a genuine counter terrorism regime and that without the interference and pressure by the Security Council the counter terrorism conventions would have been left as dead letters.[162]

Another point that should be raised is the fact that the debate preceding Security Council Resolutions is by and large shorter than the one accompanying

---

[155] Article 25 sets forth that: "*The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter*."

[156] Trahan, *supra* note 36, at 239. *See also* Payal K. Shah, *Assisting and Empowering Women Facing Natural Disasters: Drawing from Security Council Resolution 1325*, 15(3) COLUM. J. GENDER & L. 711, 716 (2006).

[157] Resolution 1373, *supra* note 18, U.N. Doc. S/RES/1189.

[158] Trahan, *supra* note 36, at 240.

[159] Ian Johnstone, *Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit*, 102 AM. J. INT'L L. 275-308 (2008).

[160] Justin S. Gruenberg, *An Analysis of United Nations Security Council Resolution: Are All Countries Treated Equally?*, 41 CASE W. RES. J. INT'L L. 469-511 (2009).

[161] Eric Rosand, *The Security Council as "Global Legislator": Ultra Vires or Ultra Innovative?* 28 FORDHAM INT'L L.J. 542, 544 (2005); Shah, *supra* note 156, at 717.

[162] For further elaboration on the role of the Security Council in strengthening the counter terrorism conventions *see* Rosand, *supra* note 160.

the drafting and adoption of a treaty.[163] It could take years for states to draft a convention for the suppression of cyberterrorism, and who knows how much time will pass before the Draft Convention will be finalized. A Security Council resolution by itself could be an effective tool in the short run, although it does not have the substance to create a full international counter cyberterrorism instrument. Thus, issues of cardinal importance like those discussed with regard to the Draft Comprehensive Convention could be left unaddressed for the sake of adopting the resolution.

V. CONCLUSION

The international community has a rare and unique opportunity to take a preventive approach and create the legal framework that will make sure the international community is prepared for the "day after" a cyberterror attack. Many leaders of western countries, as well as numerous scholars have already identified cyberterrorism as the next phase in the evolution of terrorism. It is only logical that such a threat should be treated like other manifestations of terrorism have been treated – through a clear and strict prohibition under international law.

Characterized by some distinctive features, cyberterrorism presents international law scholars with the challenge of whether the current counter terrorism regime is sufficient or whether new instruments should be developed. The language of the counter-terrorism conventions which were examined developed along with time. From a relatively narrow terminology in the Montreal Convention the law evolved to include phrases such as "any other device" or "any means" in the Bombing Convention. The latter allows more flexible interpretations of the legal conditions that are to be met in order to establish legal responsibility for cyberterrorists. It is conceivable that these differences stem from the rapid development of modern technologies in the last three decades that led to the understanding among the legal community that terrorism may manifest itself through these technologies. Thus, drafting of conventions became more sensitive to the need to adjust to future developments.

The applicability of these two conventions to cyberterrorism is, as demonstrated, possible. Nevertheless, as long as there is no clear prohibition on any form of use of computer infrastructure for terrorist purposes the analysis suggested above presents just one school of thought. There are other ways interpretations could exclude cyberterrorism from the scope of the abovementioned conventions. Given that my interpretation derives from the text, but is not embedded in the text, it leaves room for opposite claims. For this

[163] Trahan, *supra* note 36, at 242-243.

reason it is important to explore the options to explicitly prohibit cyberterrorism. As long as there is no clear cut prohibition on cyberterrorism in all forms and methods, then we are not as prepared to deal with cyberterrorism as we can be.

Creating a direct prohibition on cyberterror can take many forms, as discussed at length in Part IV. There are at least five other possible courses of actions that may be used to target cyberterrorism. Each of these options has advantages, as well as deficiencies, preventing any of them from being an "ultimate" counter cyberterrorism legal instrument. While some of the tools may provide a relatively efficient way, their scope is rather limited. Other tools enjoy a wider coverage but at the same time are not suitable for cyberterrorism.

A combination of the various instruments described may prove to be a better way to address the issue. Such a regime will include a clear prohibition of cyberterrorism via the Draft Comprehensive Convention or through a sectoral convention drafted for this purpose, in addition to an acute Security Council resolution under Chapter VII as well as criminalizing cyberterrorism in the Rome Statute and/or amending the Council of Europe's Convention on Cybercrime.

This course of action will allow for an expeditious filling of the current gap in international law with respect to cyberterrorism. It would enable the international community to have the direct legal basis to combat it, rather than recourse to treaty interpretation. Moreover, relying on different instruments would contribute to the legitimacy of the regime, as it will aspire to balance the binding Security Council resolution with the ability of states to comply with provisions of other conventions in accordance with the domestic legal system.

While it is left in the hands of computer experts to ensure that data protection programs will combat cyberterrorism on the technological aspect, it is in the hands of international legal experts to make sure that if they fail, and a cyberterror attack is successful, we will have the means to bring the cyberterrorists to justice.