Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

# Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime

*Pardis Moslemzadeh Tehrani*, Nazura Abdul Manap, Hossein Taji*

*Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia*

*Keywords:*
Cyber terrorism
Cyber security
Transnational crime
Cyber threats
European Convention on Cybercrime

ABSTRACT

With the widespread concerns about cyber terrorism and the frequent use of the term "cyber terrorism" at the present time, many international organisations have made efforts to combat this threat. Since cyber terrorism is an international crime, local regulations alone are not able to defend against such attacks; they require a transnational response. Therefore, an attacked country will invoke international law to seek justice for any damage caused, through the exercise of universal jurisdiction. Without the aid of international organisations, it is difficult to prevent cyber terrorism. At the same time, international organisations determine which state court, or international court, has the authority to settle a dispute. The objective of this paper is to analyse and review the effectiveness and sufficiency of the current global responses to cyber terrorism through the exercise of international jurisdiction. This article also touches upon the notion of cyber terrorism as a transnational crime and an international threat; thus, national regulations alone cannot prevent it. The need for an international organisation to prevent and defend nations from cyber terrorism attacks is pressing. This paper finds that, as cyber terrorism is a transnational crime, it should be subjected to universal jurisdiction through multinational cooperation, and this would be the most suitable method to counter future transnational crimes such as cyber terrorism.



## 1. Introduction

While the rapid growth of technology is beneficial to humanity, it has also given rise to cyber terrorism, one of the most alarming global threats. Cyber terrorism attacks have become a pressing issue due to the deficiency of a consistent international treaty and the lack of international resolve. The increasing incidents of cyber-attacks against sovereign states and their critical information infrastructures necessitate a global response. Regional and bilateral agreements and local legislation are not sufficient to deter cyber-attacks. Therefore, international law is a necessary tool to enable the global community to deter cyber threats in its various jurisdictions. In order to reach a common understanding in curbing cyber terrorism threats, the existing solutions offered by present international treaties must first be considered in order to look at available responses against transnational cyber threats. In fact, one of the main issues in dealing with cyber terrorism is the lack of international resolve.

Due to the fact that cyber terrorist attacks are conducted in multiple states, the procedure of prosecution is difficult; therefore, the attacked country will invoke international law to seek justice for damage caused. Although nations must come up with self-regulatory legal mechanisms to combat against the misuse of new technologies, such mechanisms need to be supported by international agreements and appropriate

* *Corresponding author.*

0267-3649/$ – see front matter 
http://dx.doi.org/10.1016/j.clsr.2013.03.011

national legislation.[1] This paper analyses the notion of cyber terrorism as an international crime. Consequently, the transnational nature of cyber terrorism subjects it to universal jurisdiction, and universal jurisdiction is exercised through the authority of multilateral organisations when a proper number of states accede to them. Regional organisations may act as multilateral ones if a large number of countries ratify them. An example is the Council of Europe Convention on Cyber Crime which has been ratified by many states (even more than the European Union) and has become the only international treaty against cybercrime at the current time.

### 1.1. *Is cyber terrorism an international crime?*

Although, the term "cyber terrorism" is being used with increasing frequency nowadays, an agreed-upon definition has not been arrived at. The definition of the term "cyber terrorism" has varied from being incredibly broad to being focused. If a too-narrow definition is adopted, it will exclude and lose many of the elements of large scale cyber-attacks; in contrast, a too-broad definition will include too many of the elements of actual cybercrimes under the category of cyber terrorism. In fact, however, among the countless definitions that exist for cyber terrorism, some unity exists that could contribute to our understanding of the issues pertaining to cyber terrorism.

Dorothy Denning provides an alternative definition that incorporates the type of motivation, the purpose of the attack, and the objects of the attack. She defines cyber terrorism as: "cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives".[2] The threat of cyber terrorism is recognised as having the same impact as a "normal" terrorism attack in Denning's definition.

Other scholars have also defined cyber terrorism. Pollitt defines cyber terrorism as "the premeditated, politically motivated attack against information, computer systems, and data which results in violence against non-combatant targets by sub national groups and clandestine agents."[3] He focuses on the point that an act of cyber terrorism must result in violence and describes the group launching the attack, which is not mentioned by Denning and in this way, is different from Denning's definition. Considering all appropriate cyber terrorism definitions, the conclusion is reached that the facts which differentiates cyber terrorism from other types of cybercrimes is the motivation and/or intention of the person or group launching the attack.

Cyber terrorism has been described as a new version of traditional terrorist activity and as the old offence of terrorism that is committed by using new technologies. Terrorist groups have turned from conventional attacks to cyber-attacks. They can launch their attacks from far distances and they disregard borders and physical barriers. They launch their attacks by using cyber space. Nonetheless, the result of such kind of offences can reach much further than the traditional methods and can have graver consequences than conventional terrorism. This is because the traditional terrorist attack is restricted to certain vicinity, while cyber terrorism is potentially capable of being committed over a wide area or a network through information and cyber-attacks, using computers in an area remote from the place the attack occurs.[4]

In the virtual world, cyber criminals and cyber terrorists use a computer as a tool to target other computers. Terrorists launch their attacks by using various methods. The result of some attacks does not only remain in the virtual world, but also impacts real life by the destruction of property or the loss of life.

The nature of the internet gives the ability to the user to disguise its identity, leading to inherent difficulties in determining the states that fail to prevent an attack from being originated within their borders. Therefore, states must cooperate with each other to share information in order to attribute attackers.[5] Terrorist groups have turned from conventional attacks to cyber-attacks, since they can now launch their attacks from far distances and disregard entire borders and physical barriers. Cyber space has become a fertile ground because of its lack of boundaries. In addition, terrorists can hide their identity and territorial location and remain anonymous. Therefore, they can generate fear among societies. They can cause death on a large scale and force targeted countries to abstain from doing certain acts.[6]

Finally, it is concluded from the points noted above that, the term "cyber terrorism" is an international crime and the response against such crime must be international. The transnational nature of cyber terrorism offences leads to jurisdictional complexity, and due to the difficulty arising from its prosecution and investigation, an attacked country will invoke international law to seek justice for damage caused.

## 2. International or universal jurisdiction

Universal jurisdiction is applied to crimes that are more serious.[7] These crimes come under universal jurisdiction in two ways: firstly, the heinous nature and scale of the offence, which encompasses grave breaches of humanitarian law; or secondly, because of the inadequacy of legislation by the

[1] L. Bantekas, International Criminal Law, Routledge-Cavendish Publication, 265 (3rd Edn, 2007).

[2] D.E.Denning, Statement of Dorothy E. Denning (2000), *available at* www.house.gov/hasc/testimony/106thcongress/00-05-23denning.htm.(Last Visited July. 17, 2012).

[3] M.M. Pollitt, Cyberterrorism fact or fancy?, 2 Comput. Fraud Secur (1998), *available* at http://cosc.georgetown.edu/denning/infosec/pollitt.html (Last Visited July, 17. 2012).

[4] D.E. Denning, Cyber Terrorism, 7 (2000), *available at* http://www.nautilus.org/rchives/infopolicy/work shop/paper/denning.html (Last Visited March, 13. 2012).

[5] L. Grosswald, Cyber Attack Attribution under Article 51 of the U.N. Charter, 36 Brook. J. Int'l L. 1151 (2011).

[6] C. Ernest, *Cyber Crime: New Threat and Global Response' Expert Group on Cyber Crime*, Department on New Challenges and Threats, 17–21 January 2011.

[7] S. Macedo, Universal Jurisdiction: National Court and Prosecution of Serious Crime under International Laws, at 4 (1st ed. 2006).

nations involved, these crimes are committed in territories that are not subject to the authority of any states.

Universal jurisdiction may be created by treaty regimes, or as a matter of customary international law.[8] Treaty regimes are binding on the states that are parties to them. However, in certain circumstances, they serve as evidence of customary international law.[9] The theory of universal jurisdiction permits the international community in prescribed jurisdictions to displace the national law with international law. Universal jurisdiction is prescribed for cyber terrorism as a matter of customary international law. Customary international law includes opinio juris and state practice. Terrorism has been considered in a number of treaties (state practice), and numerous treaties have recognised various types of terrorism. They accepted that cyber terrorism is generally a form of terrorism, despite the fact that they do not mention cyber terrorism per se, As well as this, terrorism is considered a heinous crime against humanity (opinio juris). Thus, these two elements of customary law – opinio juris and state practice – are suitable for application against terrorism and subject terrorism to universal jurisdiction.

Crimes against humanity, such as genocide and piracy, are resolved by exercising universal jurisdiction. The heinous nature of cyber terrorism as a new type of traditional terrorism subjects cyber terrorism to universal jurisdiction. The heinous nature of cyber terrorism acts is also on par with genocide and other crimes against humanity which are subject to universal jurisdiction. According to the principle of universal jurisdiction, these crimes are subject to universal jurisdiction since as they are committed by a state, or a representative of state, they may go unpunished.[10] In this regard, due to the nature of cyber terrorism which is transnational and the fact that universal jurisdiction is the best method to be applied to cyber terrorism, the proper response to cyber terrorism issues must be international. By the same token, international organisations' efforts against cyber terrorism should be exerted on the basis of universal jurisdiction.

Finally, the exercise of universal jurisdiction for cyber terrorism cases must be implemented through international organisations and their tribunals such as the International Criminal Court and International Court of Justice which have been set up by the Rome Statute and the United Nations, respectively. In other words, international organisations provide a legitimate basis, through treaties, for exercising universal jurisdiction over cyber terrorism.

## 3. International organisations

Treaty laws by international organisations provide a legitimate basis for exercising universal jurisdiction over cyber terrorism particularly, the universal jurisdiction that is exercised through the international community rather than states since universal jurisdiction can be applied through both the international community and states. However, the international community has primacy over national courts in adjudicating.[11] In fact, cyber terrorism is a transnational and trans-border crime. It applies to offences across borders; therefore, the proper response that has the potential to combat cyber terrorism should be transnational. Numerous treaties have been affected on terrorism, and as cyber terrorism is a part of traditional terrorism which launches its attack via the internet, such treaties may cover cyber terrorism as well.[12] Moreover, "the ease with which the origins of cyber-attacks can be hidden, and the fact that cyber-attacks on one nation can come from anywhere on the globe, mean that cybercrime and cyber terrorism are truly international threats."[13]

During recent years, the statistics have shown that multilateral cooperation is the most effective method to respond to transnational cyber terrorism. The necessity for such cooperation comes to mind due to the fact that countries have different rules to regulate extradition, legal assistance, and substantive law that govern computer crime; therefore, the effort to prevent and respond to computer attacks must be global in order to prevent and deter cyber terrorism. In this respect, it is concluded that the most effective form of international cooperation to respond to cyber-attacks has been multilateral in nature.[14]

In simple terms, a treaty has various political consequences which may advance the underlying goals of security, deterrence from specific offences, allowing for prosecution and extradition, and consequently, enhancing the level of deterrence against cyber terrorism. In doing so, the treaties will remove jurisdictional difficulties in the investigation of the offence and thereby cyber offenders will be deterred from cybercrime and cyber terrorism.[15] In addition, the cooperation resulting from a treaty enhances the cooperation among signatory countries, as well as technical cooperation, beyond the boundaries of the treaty. Despite the fact that at the time of the creation of some of the international instruments, cyber terrorism was not considered, the general wording of them is often sufficient. Although most cyber terrorism activities are covered by such international organisations, some major problems still exist. For example, first, the number of countries that have joined and actually implemented the law is

[8] L. Nadya Sadat, Universal Jurisdiction: Myths, Realities, and Prospects: Redefining Universal Jurisdiction, 35 New Eng. L. Rev. 242 (2001).

[9] International Bar Association, Report of the Task Force on Extraterritorial Jurisdiction, 2008, at 17, available at (Last Visited May, 12. 2012). http://www.ibanet.org/LPD/Financial_Services_Section/Securities_Law_Committee/Projects.aspx.

[10] Nadya Sadat, Supra note 8, at 243.

[11] S. Wilske & T. Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet, 50 Fed. Comm. L.J. 170–171 (1998).

[12] *Supra* note 9.

[13] R. Miyawaki, The Fight Against Cyber Terrorism: A Japanese View, Paper Presented to The Centre for Strategic and International Studies (June, 29 .1999).

[14] S.Suleymasn, Cyber Terrorism and International Cooperation: General Overview of The Available Mechanisms to Facilitate an Overwhelming Task, in Responses to Cyber Terrorism 74–75(1st ed, Centre of Excellence Defense against Terrorism, 2008).

[15] A.D. Sofaer & S.Goodman, Past as Prologue: International Civil Aviation Agreements as Precedents for International Cooperation against Cyber Terrorism and Cyber Crime, in International Approaches to Cooperation against Cyber Crime and Cyber Terrorism (1st ed, Hoover Institution Press, 2003).

limited and this situation causes many problems. Therefore, only a broad international consensus can pave the way and bring success in combating cyber terrorism. Second, the lack of procedural rules for investigation and prosecution prevents possible convictions.

Countries must bind together in multilateral cooperation. In this section, the most effective organisational structures will be considered. It focuses on the efforts aimed at responding to cyber terrorism in the international arena. Although there are numerous international organisations (including multilateral, bilateral, and regional) this paper only considers the multilateral ones and the examples considered will include the European Convention on Cybercrime. Multilateral organisations will be considered because, as mentioned above, they provide the most effective methods in responding to transnational cybercrime and cyber terrorism as the key issue in dealing with cyber terrorism is the lack of an international response.

### 3.1. *United Nations*

The United Nations is the lead organisation that tries to coordinate and seek cooperation in dealing with the problem of international terrorism.[16] The main goal of the United Nations is to keep maintaining international peace and security. Nevertheless, it establishes many specialised agencies and programmes.[17] Furthermore, within Resolutions 55/63 (2000) and 56/121 (2001) on Combating the Criminal Misuse of Information Technology, the value of the Group of Eight Principles were noted.[18] Its member states are urged to consider these principles; further, there are also other Resolutions[19] calling on member states "to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats."[20]

Following the tragedy of 11 September, the UN Security Council Resolution 1373 moved forward to fight against terrorism. It declared international peace and security and imposed an obligation on all United Nations member states to support and prevent terrorism financing, as well as criminalising terrorist activity, terrorist financing, and supporting terrorist activity. It obliged all member states to cooperate with other government and international organisations to deny safe havens for terrorists. It directed efforts in different aspects of fighting against terrorism.[21] It imposes mandatory obligations to block terrorist funds, to prevent terrorist activity, to cooperate on judicial and extradition questions, and to coordinate on the related issues of transnational crime, illicit drugs and arms trafficking.[22] The UN International Convention for The Suppression of The Financing of Terrorism, which was adopted by the General Assembly of the United Nations in Resolution 54/109 in 1999, also promotes international cooperation. Requests for cooperation may not be refused on political grounds, according to Article 14 of this Convention.[23]

The United Nations set up a Counter Terrorism Committee (CTC) to monitor the implementation of Resolution 1373 and to assist nations in developing the required capabilities.[24] The CTC is known as the "centre of global efforts to fight terrorism". It has imposed sweeping legal obligations on UN member states to combat global terrorist threats. It goes beyond the other existing counter terrorism treaties (that bind those who have voluntarily become parties to them by creating uniform global obligations) by requiring every country to freeze the financial assets of terrorists and their supporters.[25]

The United Nations Security Council Resolution 1566 (2004) requires states to fully cooperate in the fight against terrorism, and Resolution 1624 (2005) calls upon states to "prohibit by law incitement to commit a terrorist act or acts".[26] Accordingly, these two Resolutions will be discussed. UN Security Council Resolution 1535 creates a Counter-Terrorism Committee Executive Directorate (CTED) to facilitate technical assistance to countries. It promotes cooperation within the UN organisations as well as cooperation among regional and intergovernmental bodies. Furthermore, it provides expert advice to the CTC in all areas covered by Resolution 1373.[27]

United Nations Security Council Resolution 1566 was constructed based on Chapter VII of the United Nations Charter which considers the act of terrorism seriously and condemns terrorism in all of its forms. It calls on states to cooperate fully with the Counter Terrorism Committee (CTC) which was established pursuant to Resolution 1373(2001). This Resolution provides an internationally recognised definition of "terror" for the first time which seems to provide an inclusive ban on all forms of violence that internationally target civilians, regardless of the motive, as well as calls on countries to prosecute terrorists.

Resolution 1617 (2005) calls on states to combat terrorism in all its forms in accordance with the Charter of the United

[16] C.D. Yaman, Human Rights and Terrorism, in Legal Aspect Of Combating Terrorism 52 (1st ed. 2008).

[17] United Nations (1945) (UN), *available at* http://www.un.org/en/aboutun/index.shtml (Last Visited Sept, 22. 2011).

[18] http://www.un.org/en/aboutun/index.shtml (Last Visited May, 5. 2010).

[19] Developments in telecommunications and information in the context of international security, 53/70 (1998), 54/79 (1999), 55/28 (2000), 56/19 (2001), 57/53 (2002), 57/239 (2002), 58/32 (2003), and 58/199 (2003).

[20] L Xingan, *International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene*, 4 webology (2007),http://www.webology.ir/2007/v4n3/a45.html (Last Visited May. 13, 2010).

[21] About The Anti-Defamation League, http://www.adl.org/Terror/tu/tu_38_04_09. (Last Visited Sept, 22. 2011).

[22] Yaman, *Supra* note 16.

[23] The UN International Convention for The Suppression of The Financing of Terrorism of 1999, Un treaty series Reg. No.38349, adopted by the General assembly of the United Nations in resolution 54/109 on 9.12.1999.

[24] Ibid.

[25] E. Rosand, The UN-Led Multilateral Institutional Response to Jihadist Terrorism: Is a Global Counterterrorism Body Needed?, 3 JCSL 399 (2006).

[26] Raphael F. Perl, Head, Action Against Terrorism Unit, Org. for Sec. & Coop'n in Eur., Terrorist Use of the Internet: Threat, Issues, and Options for International Cooperation, Remarks at the Second International Forum on Information Security 2 (Apr. 7–10, 2008), *available at* http://www.osce.org/documents/cio/2008/04/30594_en.pdf.

[27] Cyber terrorism- The Use of The Internet for Terrorist Purposes, Council of Europe Publishing 90–91(1st ed. 2007).

Nations and also stresses that states must ensure that any measures taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law, in particular international human rights law, refugee law, and humanitarian law.[28] In 2008, the United Nations General Assembly adopted Resolution A/RES/2321 on cyber terrorism, focussing on enhancing public awareness and calling for a standard punishment for these types of attacks. In addition, in 2010, the General Assembly adopted a resolution on the "creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures", encouraging its member states to share best practices and measures in cyber security. The potency of a Security Council Resolution, which is legally binding and vested by Article 25 of the UN Charter, cannot be under-emphasised. It is a strong and effective implementation tool which has global application to all UN members. For instance, Resolution 1373 borrows various obligations from existing counter-terrorism conventions and applies them to all UN member states, without the need for them having to sign those conventions. What is more, a Security Council Resolution can be established in a short period of time, compared with the period of time it takes for a treaty to be adopted. Drafting a treaty between states might take many years. Considering these advantages, although a Security Council Resolution cannot create a complete international counter-terrorism instrument, it can still be a most effective tool.[29]

#### 3.1.1. *International conventions against terrorists*

According to the Vienna Convention on the Law of Treaties (known as the "Treaty on Treaties"), parties can choose to interpret sources other than the text of a treaty as long as they agree that those sources provide interpretive information that is authoritative.[30] Therefore, the text of a treaty may be expanded, either explicitly or implicitly, to cope with rapid technological changes so as to cover new circumstances and thus, legislation may be amended to reflect existing legal circumstances. In this way, most of the international counter-terrorism conventions can be applied to cyber terrorism. Although the United Nations has published charters on war and terrorism, establishing laws and conventions pertaining to cyber terrorism is a complicated process, and the UN has not created a comprehensive convention that covers all acts of terrorism as yet.[31]

However, there are 17 specific conventions (including its complimentary) and major legal instruments which deal with terrorist activities and which may be applicable to cyber terrorism. These are:

- 1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft,
- 1970 Convention for the Suppression of Unlawful Seizure of Aircraft,
- 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft,
- 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
- 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons,
- 1979 International Convention against the Taking of Hostages,
- 1980 Convention on the Physical Protection of Nuclear Material,
- 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation,
- 1989 Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
- 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,
- 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,
- 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf,
- the 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection,
- 1997 International Convention for the Suppression of Terrorist Bombings,
- 1999 International Convention for the Suppression of the Financing of Terrorism,
- 2005 International Convention for the Suppression of Acts of Nuclear Terrorism, and
- 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.[32]

For the time being, the only international UN body that specialises in dealing with cyber-attacks is the International Telecommunications Union (ITU), which has been attempting to set up a focus group to establish a minimum reference point against which network operators can access their security. The Secretary General of the ITU, Dr. Hamadoun Touré, has proposed an international cyber peace treaty, and continues to advocate this idea despite resistance to it. In addition, Dr. Touré has proposed a "common code of conduct against cybercrime" which would obligate countries to: i) protect their citizens against cyber criminals, ii) deny safe haven to terrorists or criminals within their territories, and iii) not to attack another country first.

As will be discussed in the following section, at this time, the only international treaty existing to deal with cybercrime is the Council of Europe's Cybercrime Convention, which has been signed by 43 countries (the majority of which are technologically-advanced). Meanwhile, it is encouraging to note that many other countries have initiated efforts to adopt the principles of this Convention into their own legal frameworks.

[28] A.Bianchi, Assessing the effectiveness of the Un security council's Anti-terrorism measures: the quest for legitimacy and cohesion, 17 Eur J Int Law 881 (2006).

[29] J. Trahan, *Terrorism Convention: Existing Gaps and Different Approached*, 8 New Eng.Int'l & Comp L. Ann, 215, 221–222(2002).

[30] A. Cohen, Cyber terrorism: Are We Legally Ready?, 9 J. Int'l Bus. & L.1 (2010).

[31] O. Yen Nee, International Responses to Terrorism: The Limits and Possibilities of Legal Control of Terrorism by Regional Arrangement with Particular Reference to Asean, Institute of Defence and Strategic Studies 9–10, Singapore, July 2002.

[32] UN Action to Counter Terrorism, International Legal Instruments to Counter Terrorism, *available at* http://www.un.org/terrorism/instruments.shtml (Last Visited August. 23, 2012).

In the same vein, President Bill Clinton created the Commission of Critical Infrastructure Protection in 1998, as a grouping of electricity, communications and computer bodies, whose aim is to defend critical infrastructure from physical and cyber-attacks. Subsequently, President George Bush established the National Security Agency with a large cybernetics strike force. In August 2011, the United Nations launched the African Center for Cyber Law and Cybercrime Prevention in order to monitor cyberspace and cybercrime in African jurisdictions. By the same token, in 2011 in Asia, Singapore announced the first cyber security training and accreditation programme with the view to teaching c security professionals how to defend countries from hackers.[33]

### 3.2. *Interpol*

Interpol began its efforts to improve its counter-cybercrime capacity at the international level very early. A 1981 survey of members on cyber-criminal law recognised dilemmas in application of existing legislation.[34] Based on the recognition of the legal gaps between countries and gaps between the legal framework and criminal phenomena, Interpol expanded its task to both law enforcement and legal harmonisation.[35]

As discussed above, Interpol works on international crimes. One of the main crimes under this heading is financial and high-tech crimes – such as[36] currency counterfeiting, money laundering, intellectual property crime, payment card fraud, computer virus attacks and cyber terrorism – which can affect all levels of society.[37] Interpol cooperates with law enforcement authorities in the fight against transnational organised intellectual property crime.[38]

The Interpol General Secretariat has harnessed the expertise of its members in the field of Information Technology Crime (ITC) through the vehicle of a "working party" or a group of experts. In this instance, the working party consists of the heads or experienced members of national computer crime units. These working parties have been designed to reflect regional expertise and exist in Europe, Asia, and America and in Africa.[39] The main task of the central body is to harmonise the different regional working party initiatives.[40]

Interpol created an anti-terrorism section in September 2002, in the wake of an alarming rise in international terrorist attacks, called the Fusion Task Force (FTF). Its primary objectives are to identify active terrorist groups and their membership, solicit, collect and share information and intelligence, provide analytical support and enhance the capacity of member countries to address the threats of terrorism and organised crime.[41]

Six regional task forces have been created in regions considered to be particularly susceptible to terrorist activity; Project Pacific (Southeast Asia), Project Kalkan (Central Asia), Project Amazon (South America), Project Baobab (Africa), Project Nexus (Europe) and Project Middle East.

Interpol has identified public safety and terrorism as a priority crime area and countries can benefit from Interpol's unique position in the international law enforcement community in the fight against terrorism.[42] The Interpol officials involved with the FTF are all terrorism specialists seconded from their home countries.[43] Interpol will set up the Interpol Global Complex in Singapore in 2014 which would be work as a global cooperation among law enforcements. The INTERPOL Global Complex (IGC) is being built in Singapore to cope with the INTERPOL's aims in order to act as a global reference point in the research and development. It aims to enhance INTERPOL's ability to tackle the 21st century crime in order to strengthen international policy globally. INTERPOL's supreme governing body decided to create the INTERPOL Global Complex in November 2010 and endorsed the proposal in 79th Session in Doha, Qatar. This new complex brings together east and west to serve security globally and create a global entity. The IGC headquarter is in Lyon and will be built as a complement of the general secretariat in Lyon.[44]

### 3.3. *Council of Europe Convention on Cyber Crime*

The Council of Europe's European Committee on Crime Problems created an expert committee on cyber space in 1997. This committee was assigned to address the problem "of criminal procedural law connected with information technology" cyber offences, and international cooperation in criminal law when it is necessary. The Council of Europe's Committee of Experts on Crime in Cyberspace created the Convention on Cyber Crime and the Convention has lasted for four years.[45] It is known as the first "international declaration on crimes committed via the international and other computer networks".[46] It is designed to act as a medium to control cybercrime internationally. It attempts to harmonise the criminal offences relating to computer systems and investigation procedures in different countries. Moreover, it fosters a safe haven to bring domestic criminal offences in cybercrime and member states much closer together and to use it for the most effective investigation process in these kinds of offences.

[33] M.Conway, Terrorist Use of The Internet and Fighting Back, 19 sec & info. Int J 9 (2006).
[34] S. Schjolberg et al, Computer-Related Offences (*Conference on the Challenge of Cybercrime*), Council of Europe, France, 2007, *available at* http://cybercrimelaw.net/documents/Strasbourg.pdf (Last Visited Sep. 22, 2010).
[35] Xingan, *Supra* note 20.
[36] Ibid.
[37] INTWERPOL, Financial and High-Tech Crimes, *Financial Crimes, available at* http://www.interpol.int/Public/FinancialCrimeDefault.asp (Last Visited May. 12, 2010).
[38] Ibid.
[39] INTERPOL, Information Technology Crime, http://www.interpol.int/Public/TechnologyCrime/default.asp (Last Visited May. 12, 2010).
[40] Ibid.
[41] INTERPOL, Fusion Task Force, Terrorism, *available at* http://www.interpol.int/Public/FusionTaskForce/default.asp (Last Visited May. 12, 2010).
[42] Ibid.
[43] Ibid.
[44] INTERPOL, The Interpol Global Complex in Singapore, *available at* https://www.interpol.int/Public/Icpo/IGC/igc.asp( Last Visited Aug, 20.2012).
[45] Marc D. Goodman and Susan W. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, 10 ULCA JOLT 139, 144 (2002).
[46] Ernest, Supra note 6.

The criminal offences under the Convention on Cyber Crime are divided into four categories: offences against confidentiality, integrity, and availability; computer-related offences; content-related offences; and offences against infringements and related rights.[47] The Convention seeks to pursue a common criminal policy to protect society from the threat of cybercrime. Fighting against cybercrime requires fast and instantaneous cooperative action in criminal matters.[48] The Convention seeks to achieve this goal by obtaining globalised action on computer networks and international cooperation.

During the drafting period of the Convention on Cyber Crime, the main concern of the drafters was to come up with a flexible definition which had the ability to adapt to new crimes and new technologies in the field of cybercrime such as cyber terrorism. Due to this approach, the definitions, substantive criminal law and procedures are applicable to most cyber terrorism cases, although some lack of information and procedures do exist in the Convention on Cyber Crime in relation to cyber terrorism. However, the drafters faced one problem, that is, national legislators in the various member countries party to the Convention on Cyber Crime insisted on maintaining their local definitions of criminal law. Thus, the drafters found it difficult in some areas, because states have different cultures and political views, such as on human rights, data protection, freedom of speech and other issues.[49] The drafters of the Convention on Cyber Crime thus have left the detailed guidelines to the signatories, since they thought that if the Convention resisted the wishes of the signatories, they would refuse to ratify the Convention. They offered such a solution in order for the Convention to be ratified by the most number of countries.

## 4. Regional organisations

Due to the very real threat of terrorism, and taking into consideration the shortcomings of multilateral treaties, regional conventions attempt to provide a viable and legitimate basis for the fight against terrorism. Cooperation at the national level emphasises collaboration between the public and private sectors to respond to cyber threats.

### 4.1. *Council of Europe*

The Council of Europe has concerned itself with anti-terrorism since the 1970s but its efforts were stepped up in 2001 following the unprecedented terrorist attacks on the United States.[50] The Council of Europe's activities in the fight against terrorism are built on three cornerstones:

- Strengthening legal action against terrorisms
- Safeguarding fundamental values
- Addressing the causes of terrorism[51]

The Council of Europe drew up the Convention on Cybercrime (which is considered in the "International Organisations" section as it applies internationally) and the Convention on the Prevention of Terrorism, for fighting cyber terrorism and other terrorist use of the internet. However, the serious threat of cyber terrorism is not adequately covered by either of these conventions, or by other Council of Europe conventions. Further, this deficiency is not compensated for by other international organisations.[52]

#### 4.1.1. *The European Convention on the Prevention of Terrorism*

The Council of Europe has adopted the Convention on the Prevention of Terrorism to increase the effectiveness of existing international texts on the fight against terrorism. The aim of the Convention is to strengthen member states' efforts to prevent terrorism and it sets out two ways to achieve this objective; firstly, it establishes certain acts that constitute criminal offences, namely, public provocation, recruitment and training. Secondly, it reinforces the cooperation on prevention both internally (national prevention policies), and internationally.

This Convention is a unique one in contrast with other framework decisions of the European Union, since it provides the basis of human rights against terrorism.[53] The Council of Europe's Convention on the Prevention of Terrorism suffers from the lack of general threat provisions with respect to terrorist offences. Therefore it refers itself to the existing treaties.[54] The Convention on Prevention of Terrorism criminalises and prosecutes terrorists, and this can apply to cyber terrorism as well, such as Article 5's "public provocation to commit a terrorist offence."[55] What discriminates this treaty from other treaties is it not only bans incitement but also the "public provocation" when the terrorism incident committed causes a danger.[56]

[47] Ibid.

[48] Explanatory Report of Council of Europe on Convention of Cyber Crime, Preamble, Convention on Cyber Crime, Budapest, 2001. Convention on Cybercrime, opened for signature Nov. 23, 2001, Eur. T.S. No. 185, available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[49] Shannon L. Hopkins, Convention on Cyber Crime: A Positive Beginning to A Long Road Ahead, 2 JHTL 105(2002,2003).

[50] Council of Europe, Human Rights and Legal Affairs, http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/1_General/(Last Visited May, 17. 2010).

[51] Ibid.

[52] E. Tikk & R. Oorn, Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism, in Responses to Cyber Terrorism 89–92 (Centre Of Excellence Defence Against Terrorism, ed. 2008).

[53] K. Nuotio, Terrorism as a Catalyst for the Emergence, Harmonization and Reform of Criminal Law, 45 JICJ (2006).

[54] Council of Europe, Cyber Terrorism: The Use of the Internet for Terrorist Purposes 75 (1st ed, 2007).

[55] M. Gercke et al, Terrorist Use of the Internet and Legal Response, Freedom from Fear, Aug 2011, available at http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=306:terrorist-use-of-the-Internet-and-legal-response&catid (Last Visited Aug, 10. 2012).).

[56] B. David, A Survey of the Effects of Counter-Terrorism Legislation on Freedom of the Media in Europe, European Digital Rights, Digital Civil Rights in Europe (Dec, 3. 2008). available at http://www.edri.org/edri-gram/number6.23/speaking-of-terror (Last Visited April, 23. 2012).

### 4.2. *International Multilateral Partnership against Cyber Terrorism (IMPACT)*

The International Multilateral Partnership against Cyber Threats (IMPACT), backed by the United Nations International Telecommunication Union (ITU) and the International Criminal Police Organization (Interpol), is known as the world's first global public-private partnership against cyber threats and launched its global headquarters in Cyberjaya, Malaysia on 20 March 2009.[57] IMPACT seeks to bridge the gap that exists between domestic and international spheres in countering cyber threats. It promotes greater cooperation in combating cyber threats. It will act as a centralised anti-cyber terrorism intelligence centre which allows its 191 member countries to be alerted to cyber terrorism threats such as attacks against the global financial system, power grids, nuclear plants and air traffic control systems.[58]

### 4.3. *Association of Southeast Asian Nations (ASEAN)*

ASEAN operates on a Pan-Asian approach. It forms a regional forum for matters of MLA (mutual legal assistance). The methodology of ASEAN mirrors the approach of the EU. Although the cultural and economic diversity of Asia make the process of multilateralism a little bit different, the action plan of ASEAN, with China, in cooperative operations in response to dangerous drugs, in partnership with the United Nations Drug Control Program in October 2000, illustrates that this MLA (mutual legal assistance) is responsive.

ASEAN has conducted four ministerial meetings on transnational crime and the focus was on issues of transnational crime and cooperative efforts in combating transnational crime. The first meeting that was held in Manila was on transnational crime and the meeting issued a declaration that was aimed at regional cooperation in criminal matters. It proposed substantial enhancements in regional law enforcement cooperation. The next meeting also dealt with issues on collective efforts against organised crime. However, at the third and fourth meetings, there was commitment to collaborate further against computer-related crime and calls for partnership between ASEAN and other agencies such as Interpol and the UN.[59]

One of the communities of ASEAN is the ASEAN Regional Forum (ARF) which is a security cooperation forum comprised of 28 participants. They are working to facilitate threat and vulnerability notification and focus on preventing diplomacy. On the 4th seminar of ARF cyber terrorism, the ideas concerning the rise of cyber terrorism and exchange of information was facilitated. They covered a range of cyber issue in order to include 'cooperation on cyber security within the ARF". Although, it is not a collective defence organization, it offers a mechanism to resolve disagreements to avoid conflict among member states.[60]

### 4.4. *Asia-Pacific Economic Cooperation (APEC)*

After the September 2001 terrorist attacks on the United States, APEC issued a statement on counter-terrorism and condemned these attacks and increased its efforts to collaborate to fight against terrorism.

The Telecommunications and Information Ministers of the APEC economies issued the Statement on the Security of Information and Communications Infrastructures and a Program of Action in 2002, supporting measures taken by members to fight against misuse of information. They designed six recommendations as the basis for APEC's fight against cybercrime comprising legal development, information sharing and cooperation, security and technical guidelines, public awareness, training and education, and wireless security.

After that a survey of laws was carried out by member economies – the E security task group – in 2003. Following a meeting that was held in Bangkok in 2003 the objectives of the meeting were stated to be to assist economies to develop the necessary legal frameworks to promote the development of law enforcement capacity and to strengthen cooperation between private and public sectors in addressing the threat of cybercrime. They established the role of international instruments, particularly the Convention on Cybercrime. They also emphasised jurisdictional cooperation, law enforcement construction, and the capacity building of the investigators.

The sixth APEC Ministerial Meeting on the Telecommunications and Information Industry made a declaration "encouraging all economies to enact a comprehensive set of laws relating to cyber security and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63(2000) and the Convention on Cybercrime (2001). However, economies cannot enact a unified legal instrument, because there are plenty of differences between members' economies with in the APEC."[61]

## 5. Conclusion

There is no common approach to fight against cyber terrorists and the use of the internet by terrorist groups. Instead, several solutions have been suggested. As proved above, since the cases of cyber terrorism are transnational in nature, only a broad international consensus and a global joint effort on criminalisation of terrorist actions in all of its forms, which is implemented through the exercise of universal jurisdiction of international courts is able to bring cyber terrorists to justice. Moreover, it can establish a functional legal framework encompassing all related issues that have been resolved. It is of vital importance that countries have a common legal definition for the term "cyber terrorism" in order to respond to

[57] IMPACT, available at http://www.impact-alliance.org/(Last Visited May, 23. 2010).
[58] Ibid.
[59] R. Broadhurst, Developments in the Global Law Enforcement of Cyber Crime, 29 An International Journal of Police Strategies and Management 424 (2006), available at http://dx.doi.org/10.1108/13639510610684674 (Last Visited April, 14. 2012).
[60] ASEAN Regional Forum, available at http://aseansec.org/18794.htm. (Last Visited Aug. 20, 2012).
[61] Xingan, *Supra* note 20.

such kinds of transnational crime. Legally defining "cyber terrorism" on the basis of its unique characteristics not only eases the investigation process, but also enables cooperation among countries. Taken together, it is necessary to come up with a radical approach in order to respond to the real issues that pertain to the global nature of cyber terrorism. It is submitted that the real issue is nothing more than the need for a global and concerted response in order to declare cyber terrorism an international crime against humanity.

Although many treaties exist, none of them provides a binding regulatory jurisdiction. Most of them deal with limited areas and apply at regional level. The United Nations and Interpol promote security and try to prevent and remove cyber-related crime at the international level. The most significant treaty in this case is the Convention on Cyber Crime. Although the Convention on Cyber Crime is categorised as a regional effort in combating cyber terrorism, it has a prominent role in this case as a number of countries which are located outside its region have ratified and become members of the Convention. However, the most prominent treaty in the field of cybercrime does not encompass cyber terrorism. Thus, since it does not offer personal and territorial jurisdiction covering cyber terrorism, the best thing to do would be to add a Protocol specifically relating to cyber terrorism.

Finally, the multilateral organisations aim to improve their security by harmonisation of legislation, coordination and cooperation in law enforcement and utilisation of direct and indirect anti-cyber terrorism actions. The various measures illustrated in this paper indicate the need for laws to be harmonised to prevent transnational criminals from exploiting jurisdictional and legal loopholes among countries, providing fewer opportunities for them.

**Pardis Moslemzadeh Tehrani** *(pardistehrani@siswah.ukm.edu.my), Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia.*

**Nazura Abdul Manap**, *Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia.*

**Hossein Taji**, *Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia.*