Cyber Terrorism: Issues in Its Interpretation and Enforcement

Nazura Abdul Manap and Pardis Moslemzadeh Tehrani

***Abstract*—Cyber terrorism is a term which represents an act of terrorising using cyberspace as a medium. This phrase is controversial as there is no exact meaning of it. Generally, it is known as "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives". The obvious dissimilarity between cyber terrorism and ordinary terrorism is its transborderless nature. Despite of that specific characteristic, the common challenge faced by both types of terrorism is the lack of definition on what terrorism is. What more to offer specific description on cyber terrorism, as it involves technical discrepancies and ambiguous legal interpretation. With the uncertainty nature of cyber crimes and its transborderless characteristic, the concerted effort from various related organisations are needed to solve problems brought about by this crime. Thus, this paper is aimed at: to explore the existing definitions of cyber terrorism and; to look at the current action taken by the relevant organisation in combating this issue.**

***Index Terms*—Cyber, terrorism, interpretation, international effort.**

I. Introduction

Cyber terrorism is a tempting occasion for terrorist group as they would require less people, money and fewer resources. Moreover, it enables the terrorist to remain anonymous, since it is being carried out far away from actual place. Also, it enables terrorists to conduct their operations with little or no physical risk to themselves. Cyber terrorism is consisting of physical terrorism and cyber terrorism. Cyber terrorist is exploiting technology via the Internet to implement their terrorist purposes.[1] Cyber-terrorism is a new and somewhat unclear concept. However, there are so many debates behind this vague term. The debates arise from the issue whether cyber terrorism is a separate phenomenon, or just a part of information warfare practiced by terrorists.[2]

II. Interpretation of Cyber Terrorism

Cyber Terrorism is closely related to the act of terrorism. Therefore, the terms terrorism and cyber terrorism are both important to be defined.

A. Terrorism

Generally the term terrorism can be defined as any concerted action or threat of action undertaken in order to bring fear. No common understanding of this notion has been reached at an international level. However, various concerned agencies in different countries cannot create a uniform definition of terrorism.[3] National academic committee on criminal justice and global which was formed in the United States by law enforcement assistant administration classified terrorism into six categories, ie, civil order, political terrorism, non- political terrorism, quasi-terrorism, limited political terrorism, official or state terrorism. Terrorism has been an important agenda for the United Nations for decades. Thirteen conventions have been dedicated to address different aspect of terrorist activities. However, these conventions focus only on illegalizing terrorist activities and ignore the need to provide a consensus on the term "terrorism". In contrast to different definition before the 11th September, definitions after 11th September provide three general legal elements for action to be considered as terrorism. It states that "any action constitutes terrorism if it is (1) intended to cause death or serious bodily injury to (2) civilians or non-combatants with (3) the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act".[4]

B. Cyber Terrorism

Cyber terrorism has become a serious threat to national and international security, as cyber terrorists seek to advance religious or political agendas.[5] There is no single common definition of the term terrorism gained universal acceptance. Likewise, no single definition of the term cyber terrorism has been universally accepted. As a matter of fact, scholars who are expert in this field define cyber terrorism with different focus. In this research the definition of cyber terrorism is divided into intent based and effect based. Most of the experts prefer intent based of attack to qualify as the cyber terrorism, instead of effect based attack.

The term cyber terrorism combines two greatest fears of this century: cyberspace and terrorism. It refers to unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Furthermore, an attack should result in violence against persons or property, or at least cause enough harm to generate fear, to qualify as cyber terrorism. For instance, attacks that leads to death or bodily injury, explosions, or severe economic loss and serious attacks against critical infrastructures depending on impact.

Manuscript received February 15; revised April 24, 2012.

N. A. Manap is an Associate Professor in the Faculty of Law, The National University of Malaysia (UKM), 43600 Bangi, Selangor, Malaysia.

P. M. Tehrani is a PhD candidate in the Faculty of Law, The National University of Malaysia (UKM), 43600 Bangi, Selangor, Malaysia

Therefore, if attacks interrupt nonessential services or would not put a heavy burden on government, it could not qualify as cyber terrorism.[6] More comprehensively, cyber terrorism refers to 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".[7]

In the Federal Government, the FBI describes cyber-terrorism as: "Cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda." [8]

Another definition by Kevin Coleman, a former chief strategist at Netscape who writes a Homeland Security focused column for *Directions* magazine is: "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives Or to intimidate any person in furtherance of such objectives."[9]

According to Ron Dick, Director of National Infrastructure Protection Centre (NIIPC) in 2002, cyber terrorism means "any criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies".[10] Conway defines the term cyber terrorism as "premeditated, politically motivated attacks by sub-national groups or clandestine agents against information, computer systems, computer programs, and data that result in violence against noncombatant and targets".

Thus, he excludes cybercrime activities, stealing credit card information, sending emails with pornographic content, or hacking a web site. He emphasizes on political motivation which occur via computer tools ending in violence. Some researchers believe that an act is cyber terrorism only if the act results in destruction, death, and/or injury, and creates fear among the public.[11] But, it is normally not acceptable, if there is no distinction between cyber crime or computer crime and cyber terrorism. On the other hand, some also suggest that cyber terrorism does not exist at all, because they claim that the destructive aspect of cyber terrorism has not occurred yet.[12] However, this statement cannot be claimed anymore, since so many attacks have been occurred during these recent years. The scientists believe that an incident qualify to be labeled as cyber terrorism, if it happens in an accurate manner. Some evidence has shown terrorist groups have been attempting to make an attack on information infrastructure and communication network by using cyber terrorism.

One theory in previous years claims terrorist groups do not have enough expertise to launch new cyber attack. Thus, it gives the western countries the comfort of thinking that they are safe. However, it is not applicable now, because most of the country's main strategies are to empower their own basement in combating to cyber terrorism, due to the fact that they acknowledged completely about the threat of cyber terrorism.

Effects-based Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.[13] Some security experts define cyber terrorism based on the effect of an attack. They included activities that computers are targeted and the resulting effects are destructive or disruptive enough to generate fear potentially comparable to traditional act of terrorism, even if not initiated by criminals with no political motive. According to effect base definition even computer attacks that are limited in scope, but lead to death, injury, extended power outages, airplane crashes, water contamination, or major loss of confidence for portions of the economy, are defined as cyber terrorism.[14] A physical attack using the internet as a medium, it focuses on the physical destruction of information hardware and software. It happened after an unauthorized access and it executed either through use of conventional weapons or through direct manipulation of wiring or equipment. A good example of this was the disruption of nation air traffic control system, overriding the railroad signals leading the crash of two trains together, interfering with the control systems for water or electricity, or blocking and falsifying commercial communications to cause economic disruption.[15]

It should not be forgotten that the single term of terrorism and cyber terrorism have not reached to a universal acceptance. Furthermore, due to the difficulties of to determine the intent, identity or the political motivations of a computer attacker, labeling a computer attack as "cyber terrorism" is difficult.[16] It is demonstrated in the above discussions that scholars who are expert in this field define cyber terrorism with different focus.

III. International Effort in Combating Cyber Terrorism

International cooperation in order to confront with cyber terrorism has different form of relationship among government and law enforcement agencies. The cooperative efforts are divided into three types: international and global effort, multilateral and multinational effort and regional effort.

A. Effort from International and Global Organization

1) United Nation

United Nation is the lead organization which involves in the coordination and cooperation relating to the problem of international terrorism.[17] In their resolutions, they require the 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. These resolutions have the same motive to improve the cyber security awareness at both the international and the national levels.[18] However, following the tragedy of 11 September the Security Council resolution 1373 moves forward to fight against terrorism. The aim of this resolution is to counter terrorism effort. This resolution provides an internationally recognized definition of terror for the first time which seems to provide an inclusive ban on all forms of violence that international target civilian, regardless of the motive, as well as calls on countries to prosecute terrorists.

2) Interpol

The basement of Interpol is to prevent and combat international crime even where diplomatic relations do not exist between particular countries and it works on the gaps between the legal framework and criminal phenomena. Interpol has created an anti- terrorism section in September 2002 in the wake of alarming of international terrorist attack which is called Fusion Task Force (FTF). The primary objectives are to: identify active terrorist groups and their membership, solicit, collect and share information and intelligence, provide analytical support, enhance the capacity of member countries to address the threats of terrorism and organized crime.[19] 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.

B. Effort from Multilateral and Multinational Organization

1) The Commonwealth Nations

Commonwealth nation main task is to harmonize their laws of its member states. It creates the Model Law on Computer and Computer Related Crime and had a great impact on the domestic legislation. It expands criminal liability including reckless liability for the offences of interfering with data, interfering with computer systems, and using illegal devices. Also, it covers the problem of dual criminality by condemning the act which has done by offender oust side his territorial nationality, if he does an offence under a law of the country where the offence was committed. Another task of the commonwealth is to consider the legal mutual legal assistant between commonwealth member and also between commonwealth member and non commonwealth. The commonwealth law minister proposes to member state to take the convention on cybercrime as a basis for mutual legal assistance between Commonwealth member states and Non-commonwealth States.[20]

2) The Group of G 8

The group G8 is an informal forum and so it lacks an administrative structure compare with international organization. The group of G8 was originally formed in 1975 with six members and it was known as the G6. Canada then joined in 1975 and Russia became a formal member in 1998. The leaders from the United States, United Kingdom, France, Germany, Japan, Canada, Italy, and Russia have been meeting annually since 1975 to discuss issues of importance, including crime and terrorism, and the information highway.[21]

3) Organization for Economic Cooperation and Development (OECD)

The OECD is a unique forum where the governments of 30 countries work together to address the economic, social and environmental challenges of globalization. The OECD has been working for many years on a range of policy issues associated with the information society. These include infrastructure and services, consumer protection, privacy and security, through to broader issues surrounding ICT and economic growth.[22] The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to establish a heightened priority for security planning and management and to promote a culture of security among all participants as a means of protecting information systems and networks.[23] The aim of this guideline is to aim to develop a global culture of security through advice on policies and measures to address internal and external threats such as cyber-terrorism, computer viruses or hacking in a globally interconnected society, while preserving important societal values such as privacy and individual freedom.

C. Effort from Regional Organization

1) . European Union

After the terrorist attack to Madrid, the European Union and its members promise to do everything in their power to combat all forms of terrorism. Therefore, the European council approves the decision of European Parliament to declare 11 marches as European day commemorating the victim of terrorism.[24] By December of 2004, European council calls on member state to ratify the convention on the mutual assistance in criminal matters, its protocol and the three protocols to Europol convention. Also, their framework implement in other aspect such as, traffic data by service provider, cross- border pursuit, exchange of information on conviction for terrorist offences and etc. the council adopted necessary measures for council regulation to identify new and applicable function for the Schengen information system (SIS).[25]

2) Council of Europe

The main task of council of Europe since 1949 was to maintenance human rights, the rule of law and pluralist democracy, and is determined to combat terrorism which combats with these values. Following the unparalleled terrorist attacks in the United States, its efforts were stepped up in 2001. It tried to fight against cyber terrorism by strengthening legal action against terrorism, safeguarding fundamental values, and addressing the causes of terrorism.[26]

The Council of Europe set its focus area on cyber terrorism and the subject of CODEXTER (the Committee of Expert against Terrorism) is about cyber terrorism. It has been surveying the situation in member states to evaluate whether existing international instrument are sufficient to respond cyber threat or not.[27] The CODEXTER has concluded at the end of these meeting that the use of Internet for terrorist purposes includes several elements:

(i). attacks via the Internet that cause damage not only to essential electronic communication systems and IT infrastructure, but also to other infrastructures, systems, and legal interests, including human life

(ii) dissemination of illegal content, including threatening terrorist attacks; inciting, advertising, and glorifying terrorism; fundraising for and financing of terrorism; training for terrorism; recruiting for terrorism; as well as

(iii). other logistical uses of IT systems by terrorists, such as internal communication, information acquisition and target analysis.[28]

3) Convention On Cybercrime

The Convention put into effect in July 2004, which is the first and only international treaty to deal with breaches of law over the Internet or other information networks. This convention has not only been ratified by all European Union member states, but also it does not specifically address cyber terrorism. The Convention requires participating countries to update and synchronize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other unlawful cyber activities.[29] Indirectly, it can be applicable for cyber terrorism as well. Although the convention on cyber crime does not define the term cyber crime and cyber terrorism specifically, Article 2 to 6 mention various forms of criminal activity that are prohibited which may include cyber terrorism activities.

4) Council of Europe: 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 sets out two ways to achieve this objective: first, establish a certain acts of criminal offences, and second, it reinforces the cooperation on prevention both internally (national prevention policies), and internationally (modification of existing extradition and mutual assistance arrangements and additional means). In other words, the Convention contains a provision on the protection and compensation of victims of terrorism.

5) Asia Pacific Economic Cooperation (APEC)

APEC is a regional forum which was established in 1989 for facilitating economic growth and its goal is to strengthening the Asia- pacific community. APEC has 21 members and it has not obliged their members and decisions made within (APEC) are reached by consensus. After September terrorist attack on United States, APEC issued a statement on counter- terrorism and condemns these attack and effort to collaborate to fight against terrorism.

6) North Atlantic Treaty Organization (NATO)

NATO was founded in 1949 on the basis principle of collective defense. The parties are following the basic principle of the Charter of the United Nations. This cooperation and commitment to security continues among the members nations today. However, the Internet, cyber space and cyber crime were not in existence at the time that NATO was established.

Nevertheless, NATO has changed their political and technical requirement and improved their capabilities in the area of cyber defense. NATO has also to address new challenges and posed by terrorists and the threats to computer information systems (CIS).[30]

7) International Multilateral Parternership against Cyber Terrorism (IMPACT)

The International Multilateral Partnership Against Cyber Threats (IMPACT), backed by the United Nations (UN) International Telecommunication Union (ITU) and International Criminal Police Organization (Interpol), which is known as the world's first comprehensive global public-private partnership between governments, industry leaders and cyber security experts to enhance the global community's capacity to prevent, defend and respond to cyber threats. It has launched its global headquarters in Cyberjaya of Malaysia on 20 March 2009. It will act as a centralized anti-cyber-terrorism intelligence centre which allows its 191 member countries to be alerted on cyber-terrorism threats such as attacks against the global financial system, power grids, nuclear plants, air traffic control systems and others.

IMPACT seeks to unite the gap that exists between domestic and international spheres in countering cyber threats. It promotes greater cooperation in combating cyber threats. Impact is supported by International Telecommunication Union and it functions as an operational home for International Telecommunication Union.

IV. Conclusion

As a result, from considering the effort taken by the relevant organizations against cyber crime and cyber terrorism, we can conclude that the most significant treaties in this area are Convention On Cyber Crime and Convention On Prevention Of Terrorism. The general purpose of the Convention is laid down in the Preamble as to deter crimes against the confidentiality, integrity and availability of information systems and the misuse of such systems. The later is served as a supplement to the provisions of the Convention on cybercrime which criminalize the acts of a racist and xenophobic nature committed through information systems.[31]

References

[1] L. Carlos et al, Cyber terrorism- a rising threaten in the western hemisphere, 2006, United States Army National Guard, p 3.

[2] Cyber terrorism and cyber operation, US Army Training and Doctrine Command, 3nd Edn, pp. 17. 2005.

[3] O. Aytac et al, Responses to Cyber Terrorism, Centre of Excellence Defense against terrorism, Ankara,Turkey(ed.) , Netherland, pp. 178. 2008.

[4] M. Breakey, Cyber Terrorism: Origin and Impact, http://www.americanchronicle.com>accessed (8 Jun 2009).

[5] K. Gable, 'Cyber-Apocalypse Now: Securing the Internet against Cyber terrorism and Using Universal Jurisdiction as a Deterrent' (2010) 43, The Vanderbilt University Law School Vanderbilt Journal of Transnational Law, p 2.

[6] D. E. Denning, cyber terrorism, 2000, http://www.nautilus.org/archives/info policy/workshop/papers/denning.html>accessed (28 Oct 2009).

[7] D. E. Denning, Cyber Terrorism, 2000.

[8] H. M. Hendershot, 'Cybercrime 2003 – Terrorists' Activity in Cyberspace' http://www.4law.co.il /L373 >accessed6 Apr 2004.

[9] K. Coleman, 'Cyber Terrorism' (2003) Directions Magazine, http://www.directionsmag.com/ article php?article>accessed15 Mar 2004.

[10] S. Berinato "The Truth about Cyberterrorism" (2004) CIO, http://www.cio.com/archive/031502/truth. html> accessed (13 Apr 2009).

[11] D.E.Denning,CyberTerrorism,2000,http://www.nautilus.org/archives/info policy/work shop/paper /denning.html>accessed (28 Oct 2009).

[12] D. E. Denning, "Activism, Hactivism, Cyber terrorism: The Internet as a Tool for Influencing Foreign Policy."

[13] http://itlaw.wikia.com/wiki/Cyber-terrorism.

[14] L. Carlos et al, Cyber terrorism- a rising threaten in the western hemisphere, (2006) United States Army National Guard.

[15] Cyber Terrorism And Cyber Operation, US Army Training and Doctrine Command, 3nd Edn, 2005.

[16] C.Wilson, Computer Attack and Cyber Terrorist: Vulnerabilities and Policy Issues for Congress, CRS Report for congress.

[17] D. Yaman, the United Nation and Terrorism, legal aspect.

[18] L. xingan "international action against cyber crime: networking legal systems in networked crime scene" webology, http://www.webology.ir/2007/v4n3/a45.html >accessed 13 May 2010.

[19] Fusion task force, http://www.interpol.int/Public/FusionTaskForce/default.asp> accessed 12 May 2010.

[20] Legal and Constitutional Affairs Division Commonwealth Secretariat, Report on Law and Technology Workshop for the Caribbean 2003, Jamaica, 2004.

[21] What is the G8, http://www.g7.utoronto.ca/> accessed 10 May 2010.

[22] http://www.intgovforum.org/brief.htm> accessed 2 June 2010.

[23] http://www.intgovforum.org/brief.htm> accessed 2 June 2010.

[24] Declaration on Combating Terrorism, pp. 1-3. http://www.tmmm.tsk.tr/regulations_en.htm> accessed 2 May 2010.

[25] Declaration on Combating Terrorism, pp. 7. http://www.tmmm.tsk.tr/regulations_en.htm> accessed 2 May 2010.

[26] Council of Europe, human right and legal affairs, http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/1_General/ > accessed 17 May 2010.

[27] Council of Europe, human right and legal affairs, http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/4_Theme_Files/ > accessed 21 May 2010.

[28] Council Of Europe, Opinion Of The Committee Of Experts On Terrorism (Codexter) For The Attention Of The Committee Of Ministers On Cyber terrorism And Use Of Internet For Terrorist Purposes,http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/4_theme_files/Cyberterrorism.asp#TopOfPage> accessed 22 May 2010.

[29] C.wilson, Botnet, Cyber Crime, Cyber Terrorism:Vulnerebalities And Policy Issues For Congress, congressional research service.CRS report for congress, 2008.

[30] http://www.impact-alliance.org/> accessed 23 May 2010.

[31] Protocol of the convention on cyber crime, article1.

Nazura Abdul Manap is currently attached with Faculty of Law, Universiti Kebangsaan Malaysia (The National University of Malaysia). She was born in Segamat Johor, Malaysia on 29 September 1969. Her list of qualifications is as below: Ph.D (Law), International Islamic University Malaysia (2008), LLM (Lond), November 1996. Faculty of Laws Queen Mary and Westfield College, LL.B (Hons) (UKM), August 1993. She has been involving in the area of information technology law and intellectual property law for almost 16 years. Her expertise is shared with the public through her publications on these areas. Amongst others are "*Jenayah Berkaitan Komputer: Perspektif Undang-undang Malaysia*" (Computer Related Crimes: A Malaysian Perspective) published by Dewan Bahasa dan Pustaka, Kuala Lumpur and a text book of "*Teknologi Maklumat dan Komunikasi: Undang-undang , Etika dan Sosial*" (Information Technology: Law, Ethic and Social) published by McGraw Hill Education, Kuala Lumpur used by the students in the Faculty of Science and Information Technology , UKM. Her devotions in these fields substantiates through her continuous commitment by organizing national seminars on cyber laws in the year 2000 followed by a seminar on Intellectual property in 2001. She also contributes in encouraging public awareness of intellectual property rights and educates officers and people related to IP through her tour around Malaysia with the cooperation of Intellectual Property Training Center under Malaysian Intellectual Property Office (Mypo). Her involvement in this area has been recognized by Regional Center of Arbitration Kuala Lumpur (RCAKL) through her appointment as penalist (arbitrator) of domain name disputes resolution in 2003.

Pardis Moslemzadeh Tehrani is a PhD student in the National University of Malaysia. She obtained her M.Sc. (public law) form the Azad University of Iran Tehran branch in 2008 and B.Sc (Law) from Ferdowsi University of Mashhad (Iran) in 2005. Her research interests are cyber crime law, intellectual property law, and cyber terrorism law.