# Deakin University

Faculty of Law

# *Combating Financial Crime and Terrorism in the twenty-first Century*

By Noppramart Prasitmonthon

# *Combating Financial Crime and Terrorism in the twenty-first Century*

***By Noppramart Prasitmonthon****

Table of Contents

Introduction

*I. The General Clarification of the Topic Scope*……..

*II. What Can the Terrorist Use the Internet For?*…….

2.1 Communication, Commerce and Recruiting Members

2.2 Laundering Money and the Use of E-Money

2.3 Internet Gambling as a Source of Terrorism Funds

2.4 Cyberterorrism

*III. Emerging Issues Regarding the Use of Internet for Illegal Activities*……..

3.1 Jurisdictional Issue

3.2 Anonymity on Cyberspace

*IV.Legal Solutions and Preventative Methods*……

4.1 Anti-Money Laundering Law

4.2 Specific Legal Solutions for Cyberlaundering

4.3 The Prohibition of Internet Gambling as a Part of Combating Terrorist Funding

4.4 Technological Solutions on National Security

A Case Study of the FBI's "Carnivore"

4.5 International Cooperation

*V. Pitfalls of Extreme Anti-Terrorist Measures*…….

Conclusion

* LLB. (Thammasat), GradDip in Business Law (Thammasat), LLM..(Melbourne), MCL.(Deakin), Barrister at Law (Thailand). This paper was a part of MCL coursework in the subject of International Financial Crime at Deakin Law School, Australia.

## Introduction

***"History has shown us that as we invent new technologies, criminals are waiting on the periphery to use them…"***[1]

By the end of the twentieth century, digital technologies especially the Internet became widespread for many people to use these technologies to facilitate their daily lives in various activities such as in commerce, politics, education and entertainment. The chairman of the American Online or AOL, Steve Case, stated in 1999 that "it's doubtful that 100 years from now people will refer to the Internet century. Probably they will simply call it the 21st century."[2]

However, not only is the Internet technology used by good people for good purposes, but criminals today are also using such technology for malicious purposes such as laundering money via the Internet, carrying out terrorist activities and so on. This paper, thus, aims to examine how financial criminals and terrorists may use the Internet technology to commit financial crime or carry out the terrorist activities. It is also important to understand the nexus between the act of financial crimes like money laundering and financing terrorism as well as the ubiquitous use of the Internet alleged as a benevolent facilitator of the twenty-first century criminal.

The further aim of this paper is to find the answer of these following questions: where do terrorists get their money through the use of technology and how can governments best work together to stop them?[3] In the first part of the paper, it illustrates the general clarification of discussed scope. The second part discusses the likely scenario of financial crime, terrorism and the Internet, and identifies how crimes and terrorist acts can be used

---

1 Rajeev Saxena, 'Cyberlaundering: the Next Step for Money Laundering' (1998) 10 *Saint Thomas Law Review* 685.

2 Robert Samuelson, 'A Gigantic White Eelephent', *the Australian Financial Review on 23 January* 2003 section Opinion at p. 46.

3 Claire Lo, 'F ATF Initiatives to Combat Terrorist Financing' visited 06 December, 2002 at<http://www.oecdobserver.org/news/printpage.php/aid/717/FATF initiative to combat terrorist financing.html>

via the Internet. The third part analyzes the issue of difficulties of legal application in dealing with financial criminals and terrorists using the Internet and other digital technologies; this will look at the jurisdictional issue, the applicability of existing laws, and the issue of anonymity on cyberspace. The recommendations of possible solutions for such problems are discussed in part four. The final part gives an analysis on the pitfall of extreme anti-terrorist measures.

## *I. The General Clarification of the Topic Scope*

The scope of the paper is related to "international financial crime", "terrorism" and the Internet representing the sense of twenty-first century. With the requirement of word limit, the author needs to select specific issues regarding international financial crime and terrorism to discuss in this paper. In the area of international financial crime, the paper mainly examines the potential employment of electronic money ("e-money") and online gambling for money laundering. The paper also makes an attempt to illustrate the nexus between these new techniques of money laundering and terrorism financing. Certainly, the issue of cyberterrorism is also included for this discussion.

However, the author took an international perspective to study these issues and did not intend to examine related laws of specific countries. Related laws regarding money laundering, Internet gambling and anti-terrorism of Australia, the European Union and the United States are used for the discussion. Nevertheless, the United States are mainly utilized as a case study of combating terrorism due to its experience after September 11, 2001.

## *II. What can the terrorist use the Internet for?*

### *2.1 Communication, Commerce and Recruiting Members*

The Internet is open to governance by human instincts, including those of greed, deception, and hate.[4] Terrorist groups employ the Internet in the same manner that other people use such as for communication, commerce, and propaganda of terrorist agenda

[4] Bruce Branun et al., 'Model Statute www.commercial_terrorism.com: a Proposed Federal Addressing the Solicitation of Commercial Terrorism through the Internet' (2000) 37 *Harvard Journal on Legislation* 159.

and recruiting their members. However, their purposes for using the Internet for terrorist activities can be harmful to society and such use would be considered as a part of terrorist activities which may be a crime according to terrorist laws of individual nations. At least under the *US Patriot Act*, carrying terrorist activities is a crime.[5]

As there was a warning to America's prosecutors who must be prepared to respond to another increasingly popular tool-of-the-trade for terrorists which was the computer.[6] After September 11, 2001, law enforcement officials around the world have reported seizing evidence from al Qaeda operatives and other terrorist groups that outlined attacks on defense system computers, banking networks and other critical infrastructure networks.[7] CNN recently also reported on an investigation that uncovered a house in Pakistan used by al Qaeda exclusively for training its members in cyberwarfare and hacking, in what one official called a "cyberacademy".[8] In such situations, the Internet seems to empower terrorism in certain ways and increase the greater risk to targeted nations unless there are powerful computer programs that can check and monitor online movements of terrorists. Tough laws for abuse of the Internet are also needed in order to deter people from using it for criminal purposes.

### *2.2 Laundering Money and the Use of E-Money*

Money laundering has been described as the "life blood of any criminal enterprise that generates revenue".[9] "Dirty money" derived from illegal activities such as drug trafficking, racketeering, and corruption concealed its illegitimate source to make it appear legitimate by these three laundering processes: *placing*[10], *layering*[11], and

---

5 Deborah J. Daniels, 'Prosecution in the Post-9/11 Era' (2002) 36 *Prosecutor* 28.

6 Ibid.

7 Bruce Branun et al., 'Model Statute www.commercial_terrorism.com: a Proposed Federal Addressing the Solicitation of Commercial Terrorism through the Internet' (2000) 37 *Harvard Journal on Legislation* 159.

8 Ibid.

9 Madelyn J. Daley, 'Effectiveness of United States and International Efforts to Combat International Money Laundering' (2000) *Saint Louist-Warsaw Transatalantic Law Journal* 175.

10 The *placement* stage requires that the money to be transferred into a more flexible and legitimate form such as depositing into a financial institution.

*integrating*[12].[13] Generally, terrorists would launder "ill-gotten" money in the same way as other criminals did by following these laundering processes.[14]

In the event of September 11, 2001, several news reported that terrorists have turned to crimes such as income from trafficking in illegal drugs providing critical financial support to 12 of the 28 terrorist organizations identified by the U.S. State Department.[15] Such reports also pointed out that al Qaeda received significant financial support from the opium trade in Afghanistan.[16] As President Bush stated "It was important for Americans to know that the traffic in drugs finances the work of terror, sustaining terrorists, that terrorists used drug profits to fund their cells to commit acts of terror."[17] Thus, the government should combat terrorists by stopping flowing money of illegal activities like drug trafficking which is used to finance terrorism and other criminal activities proposing to disguise of the proceeds of drug trafficking and organized crime by blocking money launderers' activities. Accordingly, tracing and following the "money trail" has been a fundamental strategy to counter sophisticated crime and should be carefully planned in the first.[18]

There is no surprise that Australia and the United States attempt to prevent and detect illegal movements of funds by establishing specific regulatory bodies such as the

---

[11] The *layering* stage is the transfer of the funds through different accounts. This is often done by electronic transfer through offshore accounts in targeted countries having weak anti-money laundering law and have rigorous bank secrecy law such as the Cayman Islands, Panama and the Bahamas.

[12] The *integration* is the final step for money laundering processes where the funds retune into the legitimate economy. The money launder may withdraw such money on the bank account in form of letters of credit or checks and spend them in luxurious things e.g, cars, jewelry, and gold. Then, he can resell them again.

[13] Timothy H. Ehrlich, 'To Regulate or Not? Managing the Risk of E-Money and Its Potential Application in Money Laundering Schemes' (1998) 11 *Harvard Journal of Law, and Technology* 833.

[14] Ibid.

[15] Deborah J. Daniels, 'Prosecution in the Post-9/11 Era' (2002) 36 *Prosecutor* 28

[16] Ibid.

[17] Ibid.

[18] Adam Graycar and Peter Grabosky (eds.), 'Money Laundering in the 21st Century: Risks and Countermeasures' visited 15 December, 2002 at<http://www.aic.gov.au/publication/rpp/02/Index.html>

Australian Transaction and Analysis Centre ("AUSTRAC")[19] and the Financial Crimes Enforcement Network ("FinCEN") to detect such financial crimes.[20] The *Bank Secrecy Act 1970* of the United States ("BSA") and the *Financial Transaction Report Act 1988* of Australia impose the similar regulatory obligation on "financial institutions"[21] or "cash dealers" to retain records to assure that the details of financial transactions can be traced if investigators (e.g., AUSTRAC or FinCEN) need such documents for their investigation. Importantly, these financial entities are considered as providing "choke points" through which illegal funds must generally pass and as a storage of evidence of transaction and customer identities may be recorded.[22] They are required to report "significant cash transaction" or "suspicious cash transaction" which exceeds $10,000.[23]

However, this conventional money laundering enforcement is challenged by the increasing use of e-money also called e-cash, digital cash and digital money. E-money is a string of digits or encrypted electronic message of that value to be transferred over the Internet.[24] E-money is issued and sold by private companies, which can be non-bank issuers like technology companies such as Microsoft Corporation.[25] This electronic form of money or value can be stored as a computer code on a microprocessor chip of plastic cards so called "stored value cards or smart cards" ("SVCs") or on the hard drive of a

---

19 The Austrac plays a regulator and specialist financial intelligence unit focusing on anti-money laundering. It is respond for the Financial Transaction Report Act of 1988 which gives it authorities to collect, analysis and dissemination of financial intelligence. *See* also, <http://www.austract.gov.au>

20 The FinCEN was found by the Secretary of the Treasury on April 25, 1990 (Treasury Order 105-8). The new organization was responsible for the detection of financial crimes by providing analytical support to law enforcement investigations. In 1994, the agency would be given Bank Secrecy Act regulatory responsibilities. *See* also, <http://www.fincen.gov/helpfin.html> visited 21 January, 2003.

21 The word "financial institution" is used under the BSA whereas the word "cash dealer" is used under section 3 (1) of the FTRA.

22 Timothy H. Ehrlich, 'To Regulate or Not? Managing the Risk of E-Money and Its Potential Application in Money Laundering Schemes' (1998) 11 *Harvard Journal of Law, and Technology* 833.

23 Under the FTRA of Australia, the cash dealer has to report Austrac if the money transaction is exceed $10,000 Aus dollar while in the BSA of the US, the financial institution must report FinCEN if the cash transaction is greater than $US 10,000.

24 Alan Tyree and Andrea Beatty, *The Law of Payment Systems*, Butterworths, Sydney, 2000.

25 Sarah N. Welling and Andy G. Rickman, 'Cyberlaundering: the Risks, the Responses' (1998) *Florida Law Review*.

personal computer.[26] E-money can be used for online payments over the Internet, off-line payments in case of smart cards requiring specific card reader machines or in hybrid systems.[27] As the e-commerce is growing, the number of E-money users is projected to increase as well. This is because e-commerce consumers who are not ineligible to have a credit card such as minor or low-income people are seeking for alternative payments, which allow to shop and pay online as fast as credit card holders can do so.[28]

The recent features of e-money seem to satisfy Internet shoppers who do not have credit cards or do not want to pay over the Internet by credit cards because payment by e-money is quick, convenient and more importantly is almost undetectable or anonymous.[29] Furthermore the Internet is predicted to be a predominant source of online banking by the year 2020.[30] Corporations and individuals have begun to transfer funds worldwide. In the United States, the Internet banking population rose sharply from 6.9 millions in 1998 to 24.2 millions by the end of 2002.[31] Although there is no clear statistic of worldwide Internet banking population, the steadily growth of global Internet users which jumped from 16 million in 1995 to approximately 605.60 million in September 2002[32] indicates the likelihood of the growth in Internet banking consumers as well.

The globalization of Internet payment or cyberpayment with e-money posted certain concerns regarding money launderers may take opportunities to exploit national differences in security standards and unregulated new types of payments to conceal the

---

[26] Ibid. n. 25.

[27] Ibid.

[28] Gary P. Schneider and James T. Perry, *Electronic Commerce,* (2nd eds.), THOMSON LEARING, Boston, 2001, at p. 239.

[29] David Schepp, 'Money Laundering in Cyberspace' visited 29 November, 2002 at <http://news.bbc.co.uk/1/hi/business/1149984.stm>

[30] Wendy J. Weimer, 'Cyberlaundering: an International Cache for Microship Money' (2001) 13 *DePaul Business Law Journal* 199.

[31] Nua Internet Survey, 'Nua Analysis: US Online Banking Population 1998-2002' visited 23 January, 2003 at<http://www.nua.com/surveys/analysis/graphs_charts/compa…>

[32] Nua Internet Survey, 'How Many Online?" visited 23 January, 2003 at<http://www.nua.com/surveys/how_many_online/index.html>

flowing of illicit money.[33] In a tactic as old as banking itself, criminals have always used banks as sure-fire way to launder money gained through illegal means.[34] However, with the advent of Internet banking, "following the money" to locate and prosecute money launders and criminals has become more difficult than ever. Money laundering, which involves disguising the origins of illegal obtained cash and then transforming it into apparently legitimate investments, is bolstered by the near anonymity that can sometimes be achieved through Internet communication.[35]

The most concerning feature of e-money payments is that the elimination of the physical movement of large-scale cash is considered as the money launderer's biggest problem.[36] Internet payment instruments such as network-based systems of e-money and smart cards have potential for abuse by money launderers to use it to conceal the movement of illicit funds. Take one example of the street drug market where drugs would be sold to users in exchange for disposable smart cards denominated in amounts typically with street drug transaction for instant $20, $50 or $100.[37] The drug dealer would collect these smart cards and take them to a retail store. The merchant would then upload the electronic value from the smart cards from his merchant terminal to a bank or funds-holding account at a financial institution.[38] The merchant would receive a fee for the use of his value upload capabilities. Once the funds have transferred to legitimate payment system, the funds could be further transferred to a domestic or offshore account in a process analogous to the placement, layering and integration terms of conventional money laundering.[39] The movement of high-value funds in this manner could reduce risk of detection by officials or banks due to its speed and invisibility.

---

[33] The RAND, 'The Potential Exploitation of Cyberpayments systems for Money Laundering' visited 07 December, 2002 at<http://www.rand.org/publications/MR/MR965/.pdf/MR965chap4.pdf.>
[34] Ibid. n. 29
[35] Ibid.
[36] Ibid. n. 33
[37] Ibid.
[38] Ibid.
[39] Ibid.

In addition, the advance of telecommunications devices such as mobile phones enhances the ability of funds movement by allowing launderers to transfer stored value over smart card enabled telephones.[40] These funds transferred methods could be beyond the reach of law enforcement authorities, as the transferer does not have to present himself or herself in order to do the transaction. One officer from the *Financial Action Task Force* ("FATF") stated regarding this issue that "A potential risk existed at any stage of the contract between a new customer and a financial institution,".[41] The FATF also pointed out that in the case of Internet banking, the difficulties "were increased if the procedures for opening accounts were permitted to take place without face-to-face contact…"[42]

Another example of e-money abuse via Internet payment systems involves "bogus web sites" analogous to a "font business" or a "shell company" in the process of traditional money laundering.[43] This fraudulent e-business including bogus charity web sites only accepts electronic value or e-money for payment or donations. These electronic funds could be uploaded from the electronic purses on PCs to a bank account, and then redistributed from one financial institution to another individual or group elsewhere in the world.[44] Funds collected from these bogus e-businesses seem to derive from legitimate sources because the use of e-commerce tactic disguises the proceeds of criminal activities such as drug trafficking or terrorist finance. Cyberspace will thrive as a haven of e-money laundering by criminals and terrorists unless the government closely monitors "suspicious" web sites operating e-businesses and e-donations.

### *2.3 Internet Casinos as a Source of Terrorism Funds*

The United States seem to be a country most enthusiastic to prohibit the Internet gambling business due to its concerns on vulnerability of the Internet gambling industry

---

40 Ibid.
41 Ibid. n. 29
42 Ibid.
43 Ibid. n.33
44 Ibid.

to money laundering.[45] In October 2001, the US House of Financial Services committee by voting 62-1 passed an "anti-terrorism" bill that limited Internet gambling.[46] As the FBI, the Department of Justice ("DoJ") and law enforcement bodies reported that there was "a clean nexus, a connection, between Internet gambling and money laundering of terrorism activities", Internet gambling has been limited by Bill HR 3004- *the Financial Anti-Terrorist Act* of 2001.[47] The FATF expressed concerns similar to those of U.S. law enforcement authorities and identified Internet gambling as an area requiring greater regulatory scrutiny on an international as well as national level. In a February 2001 task force report of the FATF, it reported that some member jurisdictions had evidence that criminals were using Internet gambling to launder their illicit funds.[48]

It is interesting to look at some features of Internet gambling industry, how it works and how it can potentially be a money-laundering source as alleged by certain law enforcement authorities. The first Internet casino was Interactive Casino, Inc. ("ICI") which first operated on August 18, 1995.[49] The number of Internet gambling web sites is growing sharply from at least 400 offering sport-betting sites and more than 1,400 web sites offering combined casino-style games and sport-betting sites.[50] In 2001, the Internet gambling industry gained approximately two billion dollars (US) annually.[51] The figure is projected to more than six billion dollars by 2004, with half of this figure originating from gamblers in the United States.[52]

---

45 United States General Accounting Office (GAO-02-1101R) , 'Interim Report on Internet Gambling' published on 23 September, 2002 visited 14 January, 2003 at<http://www.gao.gov>

46 Wired News, 'Terror Bill Limits Gambling, Too' visited 19 January, 2003 at <http://www.wired.com/news/print/0,129,47518.html>

47 Marc Lesnick, 'Internet Gambling and Anti-Terrorist Laws' visited 16 January, 2003 at<http://www.winneronline.com/articles/october2001/bill_details.htm>

48 United States General Accounting Office (GAO-02-1101R) , 'Interim Report on Internet Gambling' published on 23 September, 2002 visited 14 January, 2003 at<http://www.gao.gov>

49 Nick Feldman, 'Internet Gambling' visited 19 January, 2003 at<http://gsulaw.gsu.edu/lawand/papers/su01/feldman/>

50 Mark D. Schopper, 'Internet Gambling, Electronic Cash & Money Laundering: the Unintented Consequences of a Monetary Control Scheme' (2002) 5 *Chapman Law Review* 303.

51 Ibid.

52 Ibid.

The ease of access, of use and the convenience of placing wagers at the online casino from the comfort of users' home are the important factors attracting millions of Internet gamblers over the world.[53] To place wagers, the gamblers are required to register and have an account with online casinos in order to gamble with such casinos. Then, the gamblers need to fund their accounts which can be done by using one or more payment methods such as credit cards, debit cards (e.g., A.T.M cards or SV smart cards) wire transfers, checks, money orders, and e-money.[54] Apart from credit cards, the electronic money transferred business such as Western Union, PayPal.com[55] and other small electronic funds transferors seems to be more widely used than other traditional payment means (e.g., checks or money orders) for funding online gambling accounts.[56] This is because the use of additional third party intermediaries allows the casino to credit or debit the gamblers' accounts immediately.[57] This indicates the close link between the e-money business and the Internet gambling industry. However, there is no clear evidence to show how many illegal or unlicensed Internet gambling web sites are operated by terrorists, and how much "ill-gotten" money is laundered via online casinos.

Nevertheless, due to the impressive capability of e-money in the movement of large-scale funds as discussed above, the popularity of Internet gambling would attract terrorists and other financial criminals to abuse Internet gambling businesses as their money laundering haven as well as funding resources. It is no doubt why the US authorities are keen to scrutinize the Internet gambling industry as a "suspicious" business and want to ban it. Nevertheless, Australia employs a less rigorous regulatory approach in regard to the Internet gambling issue, as it licenses online casinos serving under conditions that they cannot receive the gambling placement from Australians physically in the country.

---

53 Nick Feldman, 'Internet Gambling' visited 19 January, 2003 at<http://gsulaw.gsu.edu/lawand/papers/su01/feldman/>

54 Ibid.

55 As the *Unlawful Internet Gambling Funding Prohibition* Act came into force in October, 2001, PayPal is no longer to process gambling related transactions. Many online casinos offered alternative methods of payment where their customers can not make payment via credit cards or popular intermediates like PayPal.com. In such situation, gamblers can use electronic money transfers with other intermediaries such as Netteller.com, FirePay.com, and 900Pay.com. *See* also, at <http://www. casinoguide.ws> , visited 19 January, 2003.

56 Ibid. n.53

### *2.4 Cyberterrorism*

Terrorism and the Internet are related in two ways.[58] First, the Internet has become a forum for terrorist groups and individual terrorists both to spread their messages of hate and violence and to communicate with one another and with sympathizers.[59] Secondly, individuals and groups have tried to attack computer individuals and groups have tried to attack computer networks, including those on the Internet, which has become known as cyberterrorism or cyberwarfare.[60]

Cyberterrorism has been defined as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data, which result in violence against noncombatant targets, by subnational groups or clandestine agents."[61] Such an attack can take many forms: a cyberterrorist might hack into computer systems and disrupt domestic banking, the stock exchange and international financial transactions, leading to a loss of confidence in the economy. He might also break into an air traffic control system and manipulate it, causing planes to crash or collide. A cyberterrorist could hack into a pharmaceutical company's computers, changing the formula of some essential medication and causing thousands to die.[62] He or she could break into a utility company's computers, changing pressure in gas lines, tinkering with valves and causing a suburb to detonate and burn.[63]

At this point, terrorists are using the Internet as a conduit more than they are attacking it.[64] At least 12 of the 30 groups on the State Department's list of designated foreign

---

57 Ibid.

58 Anonymous, 'Terrorist Activities on the Internet' visited 07 January, 2003 at<http://www.adl.org/Terror/focus/16_focus_a.asp>

59 Ibid.

60 Ibid.

61 W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) *UCLA Journal of Law & Technology* 3.

62 Ibid.

63 Ibid.

64 Ibid. n. 58.

terrorist organizations maintain Web sites on the Internet.[65] While the US officials believed that some terrorists used encrypted e-mail to plan acts of terrorism, most groups appear to use the Internet to spread their propaganda. Former chief of operations at the FBI Buck Revell told *US News and World Report* that "As long as they don't specifically engage in criminal acts, they can do anything they want to aid and abet their activities. This is a safe haven for them."[66]

Most Internet sites of terrorist groups seek to advance the organization's political and ideological agenda.[67] For example, Islamic militant organizations also use the Internet to disseminate their anti-Western, anti-Israel propaganda. Several Internet sites created by Hamas supporters, for example, maintain the organization's charter and its political and military plans, some explicitly called for the murder of Jews.[68] Others, like the Hizb ut-Tahrir, a radical Islamic organization based in Britain, uses its web sites to provide details to the public about its regular meetings around the UK. Still others employed the Internet to raise funds; Hezbollah, for example, the pro-Iranian Shiite terrorist organization based in south Lebanon, sold books and publications through its web site.[69]

Some Israeli and US officials believe that terrorists from Hamas and Islamic Jihad used the Internet to provide specific instructions to fellow terrorists including maps, photographs, directions, codes and technical details of how to use explosives.[70] Many of these web sites linked to other web pages that are filled with gun-related, survival, paramilitary and pseudo-judicial information and stories of corruption and murder in the highest realms of the government.[71] Terrorists' web sites may also provide information on how to build bombs as well as instructions for making dangerous chemical and

---

65 Ibid.
66 Ibid.
67 Aaron Nance, 'Taking the Fear Out of Electronic Surveillance in the New Age of Terror' (2002) 70 *UMKC Law Review* 751.
68 Ibid. n. 58
69 Ibid.
70 Ibid.
71 Ibid. n. 67

explosive weapons.[72] For instance, these web sites may pose detailed instructions of how to construct a wide rage of bombs and kinds of information that can be found in violent books such as the "Terrorist's Handbook" or the "Anarchist Cookbook".[73]

According to the Bureau of Alcohol, Tobacco, and Firearms, Federal agents investigating at least 30 bombings and four attempted bombings between 1985 and June 1996 recovered bomb-making literature that the suspects had obtained from the Internet. [74] Among the many examples, in February 1996, three junior high school students from Syracuse, New York were charged with plotting to set off a homemade bomb in their school, based on plans they had found on the Internet.[75] While many have called for laws restricting the publication of bomb-making instructions on the Internet, others have pointed out that this material is already easily accessible in bookstores and libraries.[76] It is scary to think that how cyberterrorists would brainwash young people to carry out terrorist acts for them because the young victims unintentionally absorbed terrorist propaganda through the Internet.

The international community is facing new vulnerabilities of cyberterrorist activities.[77] This new threat of cyberterrorism is not fictional. The impact of these cyberterrorism acts, while materially different from traditional attacks, such as bombing or assassinations, are capable of generating higher levels of insecurity and likely a more harmful impact on society.[78] The governments need to understand new developments of terrorist movements in the cyber world and need to create the new anti-cyberterrorism law to deal with this hi-tech terrorism.

---

[72] Ibid.

[73] Bryan J. Yeazel, 'Bomb-Making Manuals on the Internet' (2002) 16 *Notre Dame Journal of Law, Ethics, and Public Policy* 279.

[74] Ibid. n. 58

[75] Bryan J. Yeazel, 'Bomb-Making Manuals on the Internet' (2002) 16 *Notre Dame Journal of Law, Ethics, and Public Policy* 279.

[76] Ibid. n. 58

[77] M. Cherif Bassiouni, 'Assessing "Terrorism" into the New Millennium' (2000)12 *DePaul Business Law Journal.*

[78] Ibid.

## *III. Emerging Issues Regarding the Use of Internet for Illegal Activities*

### *3.1 Jurisdictional Issue*

The most problematic issue in dealing with criminal activities taking place over the Internet is the jurisdictional issue. As the communication over the Internet networks seems to be borderless, information can to flow freely across political borders through telephone lines, fiber optic/cable lines, or even microwave from satellites.[79] The globalized nature of Internet causes certain problems where there are muti-jurisdictions involved in an Internet-related criminal case in which a defendant conducted criminal activities over the Internet network and caused damages to victims in other countries. This Internet-related case is an international criminal case, in which the lawyer has to consider these questions: law of which countries shall be applied, what court has jurisdiction to adjudicate the case and how the court judgment can be enforced.[80] These questions are not easy to answer due to the effect of unclear geographic borders deriving from criminal activities on the Internet or cyberspace. The emergence of cyberspace, of course, means that a crime haven no longer needs to be a conventional, land based sovereignty[81] A haven might be a "virtual country", and virtual countries have already been created. Due to inconsistency and overlapping of substantive laws among nations, criminals take advantages from the ambiguousity of cyber jurisdiction by asserting their "virtual presence" from a hosting nation where their cyber activities such as Internet gambling, uploading pornography or displaying Nazi memorabilia are not illegal.

Take one example from the issue of Internet gambling. Australia legalized Internet gambling according to the *Interactive Gambling Act 2001* which licenses Internet gambling to operate with regulatory conditions that online casinos are banned from to taking bets from Australian Internet users who physically present in Australia.[82]

---

79 De Azevedo Ferrira Franca, 'Legal Aspects of Internet Securities Transactions' (1999) 5 *Boston University Journal of Science Technology and Law* 4.

80 Ellen S. Podgor, 'International Computer Fraud: A Paradigm for Limiting National Jurisdiction' (2002) *U.C. Davis Law Review* 267.

81 Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cybersapce' (2002) *UCLA Journal of Law & Technology* 3.

82 Andrew Handelsmann, 'Australia's Legal Approach to Internet Gambling' visited 20 January, 2003 at<http://www.gigalaw.com/articles/2001-all/handelsmann-2001-09-all.html>

However, many countries including the United States[83] outlaw the operating of Internet gambling business. Of course, many US-based Internet casinos fled to the "online-casino" haven where Internet gambling is legal such as Australia, the Caribbean Island of Antigua, Belize, Costa Rica, Curacao, Dominican Republic, Grenada and Liechtenstein.[84] The accessibility of the Internet makes it difficult to block an activity that is legal in some countries. Despite of prohibition of Internet gambling, US citizens, Chinese, Australians and people from elsewhere in the world can bet online with an online casino licensed under the government of Antigua without worrying about the legality of this Internet activity. Although there are unregulated gambling web sites operating offshore, the Internet-gambling opponent like the US might have no jurisdiction to impose its laws on other nations. As long as there are nations willing to be host to online casinos, law enforcement officials worldwide will be fighting against stacked odds.[85]

Likewise, certain nations might also be willing to become a "cybercrime haven" regardless of economic benefit.[86] The very obvious example is the preference of political benefit and the likelihood is where a country offers to shelter the activities of terrorists who use computer technology to carry out their activities.[87] There various assumptions regarding motives of the host nation of terrorists in the case of no monetary benefit

---

[83] Internet gambling is banned in the US according to these legislations:

1) The Wire Wager Act, section 1084
2) The Organized Crime Control Act 1970
3) The Bill, HR 556 the Unlawful Internet Gambling Funding Prohibition Act 2001
4) The Internet Gambling Prohibition Act 1999
5) The Money Laundering Control Act 1986
6) The Racketeer Influenced and Corrupt Organizations (RICO) Act 1970
7) The Travel Act
8) The Interstate Transportation of Wagering Paraphernalia Act
9) The Communication Act 1934

*See* also, Nick Feldman, 'Internet Gambling' visited 19 January, 2003 at <http://gsulaw.gsu.edu/lawand/papers/su01/feldman/>

[84] J.D. Tuccille, 'Smart Bet on the Net' visited 29 November, 2002 at<http://www.free-market.net/spotlight/gamble/>

[85] Jon Mills, 'Internet Casinos: a Sure Bet for Money Laundering' (2000) 19 *Dickinson Journal of International Law* 77.

[86] Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cybersapce' (2002) *UCLA Journal of Law & Technology* 3.

[87] Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cybersapce' (2002) *UCLA Journal of Law & Technology* 3.

involved; a sense of loyalty, of identification of the terrorist group's agenda and sympathizing with the terrorists might be counted.[88] Again, cyberterrorism also poses even more sensitive and problematic issues where the identification of "terrorists" among nations is different, as one nation may consider an aggressive political fighter as non-terrorism whereas the other consider it a terrorist. Nevertheless, terrorists nowadays would use this gray area of legal loophole of international laws to undertake their terrorist activities over the Internet.

### *3.2 Anonymity on Cyberspace*

Anonymity on cyberspace can cause critical problems to law enforcement officials in the process of investigation of cybercrime activities. The advance of encrypting technology allows Internet users to protect their privacy from unauthorized persons to access personal or confidential information. Encryption is a technical and complicated mathematical subject.[89] Encryption techniques are based on formulas that substitute a symbol for the true letter, number, or symbol being communicated. The specific formula, called the "key" is used to code or encrypt a message. If a person knows the key, he or she can unlock or decrypt the code.[90] Strong encryption techniques allow businesses and consumers in the digital world to have confidence that the information they are sending is secured. The private sector is building stronger and better encryption devices into their systems to ensure reliability and authenticity.[91] In particular, financial institutions and the e-money industry employ the powerful encrypting technology to ensure customers' privacy as well as prevent fraud and hacking from cyber criminals.

The e-money pioneer, for example, DigiCash,[92] were said to use the technology of encryption which was so powerful that it cannot keep track of how its customers spend

---

88 Ibid.

89 Sarah N. Welling, 'Cyberlaundering: the Risks, the Responses' (1998) *Florida Law Review* 295.

90 Ibid.

91 Ibid.

92 DigiCash is an Amsterdam-based found in 1990 by the well-known encryption creator, David Chaum. Unfortunately, the company went bankrupt in 1999.

their money.[93] Nevertheless, encryption could help money laundering. Some encryption devices are almost undecipherable and could help facilitate criminal activities.[94] Cryptographic technology allows an Internet user to send anonymous messages. Encryption software could make it almost impossible for the government to trace financial transactions.[95] According to the American Bankers Association, "military-grade cryptography plus anonymous re-mailers plus fully anonymous digital cash plus bad guys equals perfect crimes."[96]

However, technology like this creates problems for the government, which needs to be able to decrypt these messages when criminal activity is suspected. Strong security systems that protect data also can make it harder to gather the information necessary to detect money laundering.[97] Some cryptographic algorithms are almost impenetrable and are more protected than currency. Janet Reno stated that "our goal must be to encourage strong encryption for privacy in commerce while preserving law enforcement's ability to protect public safety and national security." [98] Encoding the cash where only the government or a trusted third party could read and understand it is one way to provide privacy and meet law enforcement's needs. The government's right to use the information from this "clipperized cash" could have build-in safeguards to prevent abuse.[99]

We can envisage from the emerging technology that the Internet banking industry will greatly facilitate the money laundering process for launderers to insert illegitimate money into the stream of international commerce, to wash it, through legitimate businesses and

---

[93] Ibid. n. 89
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Ibid.
[99] Ibid.

to conceal its origin, and then to withdrawn the money, ready to be spent.[100] The nature of the Internet and the strong encryption allow transactions to occur with almost no trail to follow. Furthermore, traditional financial institutions seem to be less involved in the e-money field; thus, there are no red flags altering the law enforcement to the possibility of criminal activity.[101] In order to curb cybercrime and the cyberterrorist, the government would need to consider seriously whether it should take control the use of encrypting technology of the private sector or let alone the development and the employment of the encrypting tools to the private sector.

## *IV. Legal Solutions and Preventative Methods*

### *4.1 Anti-Money Laundering Law*

Money laundering is the first target that the governments need to strengthen their anti money laundering laws to combat international financial crime and terrorism.[102] It is worthwhile to consider the high value of worldwide money laundering which seems to be a good indicator of the loose monitoring on terrorist financing. The world value of laundered funds has been estimated to be between US$500 billion and US$ 1 trillion. It is also estimated that the Asia-Pacific Region is responsible for 25 percent of the worldwide value of laundered funds. In Australia, it is estimated that between $A2 billion and $A 3.5 billion of criminal assets are laundered each year.[103]

The provoking concern of close nexus between money laundering activity and terrorism is showed in one of the first responses in the United States to the September 11, 2001 to freeze the assets of organizations linked to *Al-Qa'ida*.[104] On September 23, President Bush announced "the first strike in war against terror" by issued the *Terrorist financing Executive Order 13224*, which imposed financial sanctions on a list of proscribed

---

100 Jon Mills, 'Internet Casinos: a Sure Bet for Money Laundering' (2000) 19 *Dickinson Journal of International Law* 77.

101 Ibid.

102 Nathan Hancock, 'Terrorism and the Law in Australia: Supporting Materials' visited 26 January,2003 at <http://www.aph.gov.au/library/pubs/rp/2001-02/02rp13.htm>

103 Ibid.

104 Nathan Hancock, 'Terrorism and the Law in Australia: Legislation, Commentary, and Constraints' visited 26 January, 2003 at<http://www.aph.gov.au/library/pubs/rp/2001-02/02rp12.htm>

organizations."[105] As the US law enforcement officials believed that the September 11 terrorists had been given enough money for their terrorist preparation for many months otherwise years, they took serious step to clamp down on terrorist fund raising and money transfers.[106] On October 16, 2001 President Bush signed a new law, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* ("the *Patriot Act*"), intended to grant law enforcement officials a more powerful arsenal in the fight against terrorism.[107]

This new anti-terrorism law aims particularly on search and seizure, money laundering, foreign asset control and immigration.[108] The most affected business from the law is financial services industry (both bank and non-bank institutions), providers of electronic communications services, such as telecom companies and Internet service providers ("ISPs").[109]

Of course, the e-money suppliers would not get away from the Patriot Act if they have assets located in the United States. This is because Part II of the Act requires foreign financial institutions with assets in the United States, which never before had been directly subject to US financial regulation, to accept broad new anti-money laundering obligations as a condition for doing business in the United States.[110] The *Patriot Act* clearly established long-arm jurisdiction over money laundering by considering merely if any part of a money laundering process takes place in the United State or if the foreign person is a financial institution with a bank account at a financial institution in the United States.[111] Furthermore, domestic and foreign banks that fail to comply with the high

---

[105] Ibid.

[106] Taylor X. Francis, 'Seminar on Preventing Terrorism and Organized in the Tri-Border Area' visited 07 January, 2003 at <http://www.state.gov/s/ct/rm/2001/7012pf.htm>

[107] Debra D. Bernstein and Jonathan Winer, 'Business Implications of the U.S. Anti-Terrorism Law' visited 07 January, 2003 at<http://www.gigalaw.com/articles/2001-all/berstein-2001-all.html>

[108] Ibid.

[109] Ibid.

[110] Ibid.

[111] Ellen S. Podgor, 'International Computer Fraud: A Paradigm for Limiting National Jurisdiction' (2002) 35 *U.C. Davis Law Review* 267.

standards under the Act to prevent money laundering would be fined $US 1million per violation.[112]

In Australia, the similar anti-terrorism acts regarding the prevention of money laundering activities is also reinforced by the adoption and ratification of the *UN international convention for the suppression of the Financing of Terrorism of 1999* on October 21, 2001.[113] This Convention is implemented through the Suppression of the *Financing of Terrorism Act 2002*. It stated that countries would take action against people or countries that provide or collect funds for terrorist purposes. [114] Financing of terrorism is also criminalized in the *Australian Criminal Code*.[115] This will include collection, receipt, use and provision of funds for the preparation and planing of terrorist activities. Knowingly assisting in any of these activities is also an offence. A maximum penalty of 25 years imprisonment will be imposed for the offences.[116]

To safeguard Australia from funding terrorism, the *Financial Transaction Reports Act 1988* is amended to ensure the reporting of possible terrorist-related transactions and international funds transfers.[117] The amendment of the Act made it possible for AUSTRAC to share financial transaction reports information with other countries and the Australian Security Intelligent Organization ("ASIO") and the Australian Federal Police ("AFP"), subject to appropriate monitoring and approvals, to share such information with equivalent foreign authorities.[118]

---

112 Ibid.

113 Parliament of Australia, 'Internet Resource Guide: Criminal Law Resources' visited 26 January, 2003 at<http://www.aph.gov.au/library/intguide/law/criminalaw.htm>

114 United Nations Treaty Collection: Convention on Terrorism, visited on 26 January, 2003 at<http://untreaty.un.org/English/Terrorism.asp>

115 Daryl Williams, 'New Release from Attroney-General: Upgrading Australia's Counter-Terrorism Capabilities' visited 26 January, 2003 at<http://www.law.gov.au/ministers/attorney-general/mediamn.html>

116 Ibid.

117 Ibid.

Unlike the anti-money laundering under the *US Patriot Act*, Australian counter-terrorism measures regarding anti-money laundering do not create the long-arm jurisdiction over foreign financial institutions other than the request for cooperation. However, the Australian common law generally accepted that the States may enact laws having an extraterritorial effect so as to secure "peace, order, and good government" of the States.[119] In the future, Australia might consider establishing the extraterritorial jurisdiction in its anti-terrorism laws in order to protect Australians affected from terrorist activities occurring overseas such as the event of Bali bombings of 12 October, 2002. The Howard Government has not yet decided in this issue.

### *4.2 Specific Legal Solutions for Cyberlaundering*

The European Union seems to be most clear in its regulatory methods to deal with the e-money issue. Its directive 2000/46/EC is aimed to establish standards for a uniform EU-wide licensing scheme for institutions that issue stored-valued devices and other forms of e-money.[120] Under the directive, only credit institutions, or institution involved in "receiving deposits or other repayable funds and… granting credits" will be permitted to issue e-money.[121] E-money entities are required to meet certain regulatory requirements under the directive 2000/46/EC such as must have minimum starting capital of 1 million Euro, and 2 percent of the entity's financial obligations must be made up of its own funds.[122] Currently, some EU states permit only banks to issue e-money.[123] As the directive places certain limitations on investment by such entities and requires sound and

---

118 Daryl Williams, 'New Release from Attroney-General: Upgrading Australia's Counter-Terrorism Capabilities' visited 26 January, 2003 at<http://www.law.gov.au/ministers/attorney-general/mediamn.html>

119 Nathan Hancock, 'Terrorism and the Law in Australia: Supporting Materials' visited 26 January, 2003 at<http://www.aph.gov.au/library/pubs/rp/2001-02/02rp13.htm>

120 BNA.com, 'EC Directive Sets Standards for E-Money Issuers' (2000) 5 BNA *Electronic Commerce & Law Report* 1125.

121 BNA.com, 'EC Directive Sets Standards for E-Money Issuers' (2000) 5 BNA *Electronic Commerce & Law Report* 1125.

122 BNA.com, 'Spain's Adoption of E-Money Lagging, but M-Commerce Initiative May Change That' (2002)7 *BNA. Electronic Commerce & Law Report* 557.

123 BNA.com, 'Spain's Adoption of E-Money Lagging, but M-Commerce Initiative May Change That' (2002)7 *BNA. Electronic Commerce & Law Report* 557.

prudent management, this would make it difficult for criminal or terrorist groups who intend to launder "ill-gotten" money through the e-money channel.

It is important that the government should not leave the e-money industry to be unregulated. To prevent cyberlaundering through the use of e-money, the government needs to put forward tough regulations and closely monitor this hi-tech financial industry. In fact, before the attack of September 11, there was a debate in the United States in regard to whether the electronic payments industry should be regulated as strictly as the bank. However, such issues seem to be undisputed, as bank or non-bank institutions are in the same position to comply with the anti-terrorism provisions regarding money laundering activities under the *Patriot Act.*

With the main concerns in the increasing use of smart cards, e-money and Internet banking, the Financial Action Task Force ("the FATF") made a uniform of regulatory which recommended financial regulators to remedy this situation and prevent the use by organize crime of the new payment technologies.[124] The FATF recommended that authorities:

- Limit the functions of smart cards, including maximum value and turnover limits, as well as the number of smart cards issued per customers;
- Link all new payment technologies to financial institutions and bank account;
- Require standard record-keeping procedures for these systems, to enable the examination, documents, seizure of relevant records by investigating authorities; and
- Establish international standard for these measures.[125]

At least, the FATF guidance in relation to e-money would be useful for some countries with less experience and knowledge in handling the cyberlaundering issue.

---

[124] BNA.com, 'European Single Currency, Internet Pose New Money Laundering Worries' (1999) 4 *BNA Electronic Commerce & Law Report.*

### *4.3 The Prohibition of Internet Gambling as a Part of Combating Terrorist Funding*

Aside from new payment technologies, the FATF report also expressed concern that Internet gambling may become a new outlet for money laundering.[126] The activity which generated revenues topping $1.5 million per month in the Pacific Islands of Western Samoa, Nilue, Vanuatu, and Fiji, "represents a major new business trend… and a potential vulnerability for money laundering and financial crime in those jurisdictions" FATF stated.[127] Nevertheless, the FATF did not give any recommendation on whether of not the government should deal with the Internet gambling industry. This left individual governments to decide an appropriate approach on this issue for themselves. As discussed above, it is no doubt that the difference of substantive laws among nations in relation to Internet gambling activities creates a "legal loophole" as well as the "online casinos haven" where some countries legalize this industry and are willing to be host countries of these virtual casinos.

Currently, the United States seems to be the only country that explicitly prohibits the operation of Internet gambling businesses. The great concern of online casinos having a potential risk to be a new money laundering source, especially for terrorism resulted in the *Financial Anti-Terrorism Act 2001* comprising section 303 and 304 of Bill HR 3004 specifically dealing with Internet gambling known as "*Unlawfully Internet Gambling Funding Prohibition Act*".[128]

According to the *Unlawfully Internet Gambling Funding Prohibition Act ("the UIGFPA")*, section 303 involved "the prohibition on acceptance of any bank instrument for unlawful Internet gambling" while section 304 is related to "Internet gambling in

---

[125] BNA.com, 'Spain's Adoption of E-Money Lagging, but M-Commerce Initiative May Change That' (2002)7 *BNA. Electronic Commerce & Law Report* 557.

[126] BNA.com, 'Spain's Adoption of E-Money Lagging, but M-Commerce Initiative May Change That' (2002)7 *BNA. Electronic Commerce & Law Report* 557.

[127] BNA.com, 'Spain's Adoption of E-Money Lagging, but M-Commerce Initiative May Change That' (2002)7 *BNA. Electronic Commerce & Law Report* 557.

[128] Marc Lensnick, 'Internet Gambling and Anti-Terrorist Laws' visited 29 November, 2002 at<http://www.winneronline.com/article/october2001/bill_details.htm>

foreign jurisdictions".[129] Both provisions do not impose any liability on gamblers themselves, rather, dealing with the industry or online casino operators. Under these prohibitions, "unlawful Internet gambling is defined as the act of placing or transmitting a wager using the Internet where such a bet is illegal under state or federal law.[130] Furthermore, no person or business is allow to accept any form of payment in exchange for an unlawful online bet or wager. This also includes credit cards, cheques, wire or e-money transfers, third party intermediary (e.g., money transmitters like Western Union). Penalty for the violation is a maximum of a 5-year sentence.[131]

More interestingly, the *UIGFPA* stipulated that the US government will ask foreign government to (1) ensure that the offshore casinos do not launder money and (2) stop Internet gambling in their country and ban bets from Americans. This provision can be considered as either the request for cooperation from foreign countries or the creation of long-arm jurisdiction proposing to stop online casinos in licensed countries.[132] However, the attempt to create long-arm jurisdiction may not be a practical solution, as the globalized nature of Internet itself makes it difficult for any nation attempting to regulate. For licensed online-casino countries, high economic interest of licensing online casinos simply makes them to ignore the US request for cooperation to ban Internet gambling activities.

Nonetheless, instead of the employment of regulatory approach to prohibit Internet gambling, there are certain alternative enforcement options by focusing on obstructing a gambler's ability to access the gambling web site.[133] There are a number of techniques that can be used to prevent the access of online casinos such as filtering out Internet gambling web sites at the Internet service provider level, removing the domain name

---

[129] Mark D. Schopper, 'Internet Gambling, Electronic Cash & Money Laundering: the United Consequences of a Monetary Control Scheme' (2002) 5 *Chapman Law Review* 303.
[130] Ibid.
[131] Ibid.
[132] Ibid.
[133] Nick Feldman, 'Internet Gambling' visited 19 January, 2003 at<http://gsulaw.gsu.edu/lawand/papers/su01/feldman/>

addresses directing to Internet gambling sites, or cutting-off telecommunications services used by the web site.[134]

Deleting domain name addresses of online casinos, however, may raise a problem, as not all domain names are under control of the US jurisdiction.[135] For example, the international domain name such as ".au" for the Australian domain name or ".uk" for the UK domain name would not be legally deleted or canceled under the US law whereas there may not be any legal problem with the US government proposing to cancel the ".com" known as the US commercial domain name.[136] Thus, it is likely that the cancellation or removal of gambling web sites using the ".com" registration cannot prevent online gambling operators from transferring to use other international domain names.[137]

### *4.4 Technological Solutions on National Security*

Technology plays an important role in the national security to prevent the terrorist attack. As no government, in particular the United States, wants to be an open target of terrorism and to be attacked severely, the national security needs to be enhancing as well as more surveillance is required in the era of terrorist threat. After the September 11, President Bush spent hundreds of millions of dollars for surveillance, information-sharing and computer upgrades.[138] In fiscal year beginning October 1, 2002, the Department of Justice ("DoJ") including the FBI was granted a budget increase of $1.8 billion to a total $30.2 billion.[139] The FBI would receive $61.8 million and 201 more officers to support the agency's "surveillance capabilities to collect evidence and intelligence."[140] The US

---

134 Ibid.
135 Ibid.
136 Ibid.
137 Ibid.
138 Wired News, 'Bush Eyeballs Heavy Tech Spending' visited 24 January, 2003 at <http://www.wired.com/news/print/…>
139 Wired News, 'Bush Eyeballs Heavy Tech Spending' visited 24 January, 2003 at <http://www.wired.com/news/print/…>
140 Wired News, 'Bush Eyeballs Heavy Tech Spending' visited 24 January, 2003 at <http://www.wired.com/news/print/…>

government believed that technology would be the best solution to combat the terrorist threat. This can be seen from the *USA Patriot Act*, which gives terrorism investigators broad surveillance power to use technology devices such as the FBI's "carnivore" to intercept or wiretap electronic communications or the Internet.[141] Of course, mere anti-terrorist legislation without the employment of sufficient technology to assist the counter-terrorist measure would be useless and waste the time to pass such laws.

***A Case Study of the FBI's "Carnivore"***

The FBI's "Carnivore" is a good example of the use of technology to fight against terrorist activities in this Internet age. Carnivore is a high-speed packet "sniffer" electronic program developed by the FBI's Engineering Research Facility to conduct electronic surveillance of e-mail and Internet communications.[142] Carnivore is installed at an Internet service provider's facility to monitor certain transmissions.[143] In fact, Carnivore was made public in July 2000 according to a public request under the *US Freedom of Information Act*.[144] At that time the use of Carnivore was very controversial, as the public felt their privacy right to be invaded by the FBI and alleged that the FBI's conduct regarding the use of Carnivore might violate the constitutional law.[145]

The legality of the use of Carnivore was assured by the US Congress in the wake of September 11. This is because the *USA Patriot Act* increased the power of the DoJ to wiretap a suspected terrorist with the inclusion of "roving wiretaps" that will allow the government to track suspects regardless of the telephone or other communications they use.[146] However, the Act includes a "sunset" provision whereby some of the new

---

141 Wired News, 'How Changed Laws Changed U.S.' visited 24 January, 2003 at<http://www.wired.com/news/print/…>

142 Margaret Smith Kubiszyn, 'Legal Controversy and the FBI's "Carnivore" Program' visited 17 January, 2003 at<http://www.gigalaw.com/articles/2000-all/kubiszyn-2000-12a-all.html>

143 Ibid.

144 Mary WS Wong, 'Electronic Surveillance and Privacy in the United States After September 11, 2001: The USA Patriot ACT' (2002) *Singapore Journal of Legal Studies* 214.

145 Mary WS Wong, 'Electronic Surveillance and Privacy in the United States After September 11, 2001: The USA Patriot ACT' (2002) *Singapore Journal of Legal Studies* 214.

146 Debra D. Bernstein and Jonathan Winer, 'Business Implications of the U.S. Anti-Terrorism Law' visited 17 January, 2003 at<http://www.gigalaw.com/articles/2001-all/bernstein-2001-11-all.html>

surveillance powers will end on December 31, 2005.[147] Nevertheless, the Government assurance of the electronic surveillance does not seem to decrease the heat of debates raising by civil liberty and privacy advocates that these anti-terrorist measures may lead to abuse of power of investigators as well as erode the constitutional freedoms of ordinary citizens.[148] The argument between the US government and the civil liberty advocates like the American Civil Liberties Organization in relation to the necessity of national security and the decreasing of civil liberty to have a safer life are continuing.

### *4.5 International Cooperation*

One problem with international enforcement of anti-money laundering and terrorism measures is determining jurisdiction authority.[149] This is because the current regulatory system is based on established geographic and financial boundaries. However, international borders are less important with modern technology, thus, global cooperation and coordination is necessary to fight transnational money laundering and terrorism. For example, the governments should consider being a party of the muti-lateral convention on e-money and Internet gambling in order to prevent terrorist funding via the Internet.[150] Particularly, international cooperation is needed in the areas of extradition, mutual legal assistance, transfer of criminal proceedings, transfer of prisoners, seizure and forfeiture of assets, and recognition of foreign penal judgments.[151]

Take the Financial Action Task Force ("the FATF") as a good model of the international cooperation to combat money laundering. The FATF is a twenty-six-nation organization formed to address the international problem of money laundering.[152] The primary purpose behind the 1996-97 FATF Typologies meeting at the Organization for Economic Co-operation and Development (OECD) was to start a dialogue between FATF members and

---

147 Ibid.

148 Wired News, 'How Changed Laws Changed U.S.' visited 24 January, 2003 at<http://www.wired.com/news/print/…>

149 Ibid. n. 89

150 John Edmund Hogan, 'World Wide Wager: the Feasibility of Internet Gambling Regulation' (1998) 8 *Seton Hall Constitutional Law Journal* 815.

151 M. Cheirf Bassiouni, 'Assessing "Terrorism" into the New Millennium' (2000) 12 *DePaul Business Law Journal.*

international designers of electronic payment systems. In an attempt to fully address the ramifications that those electronic payment systems could have on international money laundering, the FATF invited private-sector representatives and banking associations to its 1996 meeting.[153]

In the issue of counter-terrorism, the FATF also cooperates with other international bodies such as the United Nations whose Counter-Terrorism Committee encourages states to participate in the FATF self-assessment exercise- the Egmont Group of the Financial Intelligent Unit, the International Monetary Fund, the World Bank and the G 20 Finance Minister and the Central Bank Governors.[154] Importantly, the FATF made a special recommendation to states regarding anti-terrorist financing to focus on: ensuring that terrorist financing is specifically listed as a criminal offence in a country's legislation; the seizure of terrorist assets; the reporting of suspicious financial transaction linked to terrorism; international cooperation; and measures to prevent the abuse of wire transfers and other remittance systems.[155] This also includes the prevention of legal entities such as non-profit organization or charitable groups from being used as a financing source of terrorists.[156] It is important to emphasize that building international cooperation is vital for success to combat terrorism in this 21st century where the world seems to be smaller due to the advance of technology like the Internet.

### *V. Pitfalls of Extreme Anti-Terrorist Measures*

The world in the post September 11 does not seem to be the same again. The governments are increasingly aware of the insufficiency of existing intellectual, moral and legal frameworks for dealing with potential terrorist attacks.[157] Several anti-terrorism

---

152 Ibid. n. 89

153 Ibid. n. 89

154 Claire Lo, 'FARF Initiatives to Combat Terrorist Financing' visited 06 December, 2002 at <http://www.oecdobserver.org/news/printpage.php/aid/717/FATF initiative to combat terrorist financing.html>

155 Ibid.

156 Ibid.

157 Tony Coady and Michael O'Keefe (eds.), *Terrorism and Justice: Moral Argument in a Threatened World*, Melbourne, Melbourne University Press, 2002.

laws were passed by many states to ensure their national security by granting even more authorities in policing, investigating and prosecuting "suspicious" people who are reported that they may be involved in the terrorist activities. There are certain pitfalls of "extreme" anti-terrorism measures. Consider the provision under the *USA Patriot Act*, for example. The US civil liberty advocates alleged that this legislation has eroded Americans' fundamental legal rights in the name of war on terror, including:

- *freedom from associations*: the government may monitor religious and political groups without evidence of criminal activity;
- *right to liberty*: Americans may be jailed without being charged or being allowed to confront witnesses against them;
- *freedom from unreasonable searches*: the government may search and seize Americans' papers and effects without probable cause to aid terrorism investigation;
- *freedom of speech*: the government may prosecute librarians, telecommunication company officials and anyone else who reveals they have received a subpoena for records related to the terrorism investigation;
- *right to legal representation*: the government may monitor penal communications between attorneys, and deny lawyers to Americans accused of crimes;
- *right to a speedy and public trial*: the government may jail Americans indefinitely without a trial;
- *Freedom of information*: the government has closed once-public immigration hearings, secretly detained hundred of people without charges, and has encouraged bureaucrats to resist requests for public records under the *US Freedom of Information Act*. [158]

This long list of the harmful effects on civil liberties and human rights deriving from the anti-terrorist law may be not profound enough to demonstrate the feeling of American people who seem to be compelled to choose either being safe or free. The justification of

[158] Wired News, 'How Changed Laws Changed U.S.' visited 24 January, 2003 at <http://www.wired.com/news/print/…>

the "extreme" counter-terrorist measures like the USA Patriot Act is doubtful. On the one hand, President Bush wanted to keep America safe, but with less freedom. On the other hand, some Americans said they were victimized by the government anti-terrorist laws, and they cannot be safe and free at the same time.[159] An outsider like Justice Michael Kirby from the High Court of Australia considered the US response to the terrorist attacks as "the error of the over-reaction". It might be the right thing to do in the preparation of national security in the wake of terrorism if the governments could "keep proportion, to adhere to the ways of democracies, to uphold consitutionalism, and the rule of law".[160] As Justice Kirby also pointed out these are the ways to maintain the love and confidence of the people over the long haul.[161] Thus, every erosion of liberty should be thoroughly justified and always keep the sense of proportion.

## Conclusion

The combating of international financial crime and terrorism in the twenty-first century should be undertaken by analyzing the technology that these criminals might use carry out their activities. Also, enhancing the technological capabilities of law enforcement bodies is needed to detect or prevent these hi-tech crimes. In this century, the Internet is said to be an influential communication tool and criminals and terrorists in many ways also abuse it. Certain Internet activities discussed above such as Internet payments with e-money and Internet gambling seem to be a potential financial source which could be use for terrorists' money laundering. In fact, several nations made an attempt to regulate the Internet either by legal or technological mechanisms. It is premature to indicate the success of such mechanisms to curb criminal or terrorist activities committed through the Internet.

Probably, the best way to fight against these transnational criminal and terrorists is the "strong intention" among governments to cooperate in legal enforcement, practical

---

159 Wired News, 'ACLU Acts Against Patriot Act' visited 24 Jaunary, 2003 at<http://www.wired.com/news/print…>

160 Justice Michael Kirby, 'Australian Law, After September 11, 2001', October 2001.

assistance and technical/technological aids. Yet, it is not an easy task to create international cooperation in one specific issue like the issue of "terrorism" and let alone the employment of diplomatic skills of individual nations to create allies to combat terrorists in the Internet era.

---

161 Ibid.