VOLUME 2 | ISSUE 1 | ISSN 2456-9704

AN ANALYSIS OF CYBER TERRORISM – NATIONAL AND INTERNATIONA PERSPECTIVE

By: L. Sanmiha
From: Saveetha School of Law, Saveetha University, Chennai

ABSTRACT

This paper deals with Cyber Terrorism- National and International Perspective. Cyberterrorism 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."Cyber terrorism has been recognized as a threat at national and international level. The reason of that cyber attacks can come from anywhere on the globe and be easily hidden. This essay contains an analysis of what cyber crimes are as against cyber terrorism. The main aim of this paper is to trace out the factors that influences cyber Terrorism. Then focus shifts on analysing various issues concerned with the policy implications. This essay ends by suggesting measures to be taken to counter the threat along with a legal analysis of the threat as it affects aviation and addresses several issues, including a discussion on some national efforts at curbing the problem in some prominent jurisdictions. Responding to cyber terrorism requires special efforts and developing strategies and policies that need to be as inclusive as possible. This study is strengthened with case laws, illustrations and advanced technology.

INTRODUCTION

Terrorism has been one of the complex issues faced by governments, policy makers, analysts, and the public. The complexity of terrorism has come out not only from the definition of the concept itself but also the tactics that terrorist groups use.

As the world changes at an unprecedented pace, the types of weapons, tar- gets and the tactics of the terrorists have changed.Today, it is considerably clear that information technologies, such as computers, telecommunication de- vices, software, and the internet have been used by all terrorist organizations. In our day, almost all of the active terrorist organizations have Web sites and use several languages to reach out to more and more people.

Government, military, financial and service sectors use computer system and internet widely. As the world has become more and more reliant on technology and networked systems, not only have legitimate entities bene ted from this trend, but also illegal groups, such as terrorists, organized crime groups, and other criminal entities have been using cyber space for their own benefits. The growing dependence of societies on information technology has created a new form of vulnerability, giving terrorists the ability to approach targets such as national defense systems and air traffic control systems.

There are multiple reasons to think terrorist groups will utilize information systems as weapons of terror. Cyber terrorism is a wise choice for modern terrorists, who assess its anonymity, its potential to cause massive damage, its psychological impact, and its

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

media appeal. If we consider terrorists as rational people who calculate the necessary preparation and consequences of their actions, cyber terrorism provides plenty of opportunity for terrorists because the attacks are cost-effective and may potentially disrupt and destroy enough lives to serve their political agenda. Also, cyber space enables terrorists to at- tack multiple targets at the same time, which can increase the significance of the attack.Cyber terrorism is one of the newest national security issue in the twenty first century. The international and national legal system must adapt to this battleground.

DEFINITION OF CYBER TERRORISM

cyberterrorism 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[1] (Denning 2000).

Pollitt[2] (1997) defines cyberterrorism as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents."

To clarify the difference between information warfare and cyberterrorism, it should be understood that cyberterrorism can be a component of information warfare, in other words, information warfare encompasses cyberterrorism[3]

According to Ron Dick, Director of NIIPC in 2002, cyberterrorism 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." (as cited in Berinato, 2002).

By combining the above concepts, cyberterrorism may also be defined as the politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies." (Wilson, 2003, p. 4.)

TYPOLOGY OF CYBER TERRORISM[4]

CATEGORY	DEFINITION AND EXPLANATION
Information attacks	Cyberterrorist attacks focused on altering or destroying the content of electronic files, computer systems, or the various materials therein.

[1]Denning, Doroty E., "Cyberterrorism: The Logic Bomb versus the Truck Bomb", Global Dialogue, Volume 2, Number 4, Autumn 2000

[2]Pollitt, M.M., "Cyberterrorism: Fact or Fancy?", Proceedings of the 20 Na- tional Information Systems Security Conference, October 1997, p.285-289.

[3]Taylor, Caeti, Loper, Fritch, and Liederbach, 2004, p. 20.

[4]Ballard, J. D., Hornik, J. G., & McKenzie, D. (2002). Technological facilitation of terrorism: Definitional, legal and policy issues. American Behavioral Scientist, 45, (6), 989-1016.

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

Infrastructure attacks	Cyberterrorist attacks designed to disrupt or destroy the actual hardware, operating platform, or programming in a computerized environment.
Technological facilitation	Use of cyber communications to send plans for terrorist attacks, incite attacks, or otherwise facilitate traditional terrorism or cyberterrorism.
Fund raising and promotion	Use of the Internet to raise funds for a violent political cause to advance an organization supportive of violent political action, or to promote an alternative ideology that is violent in orientation.

WHO IS A CYBER TERRORIST?

A terrorist does not usually spend his or her entire life working at a computer. However, there are crackers and some other people who are in that business. These people are potential candidates for becoming cyberterrorists. This conversion from cracker to terrorist may be motivated by money, prestige, and/or ideology[5] (Collin 1997). However, some analysts suggest that as terrorists are becoming more familiar with technology, a new generation terrorists who are more computer-savvy may be growing, and they may focus on using this technology to carry out cyber attacks.

INTERNATIONAL EFFORTS

Offences against civil aviation, particularly with regard to unlawful interference with civil aviation relating to aircraft have been addressed in three significant occasions in the Tokyo Convention of 1963, The Hague Convention of 1970 and the Montreal Convention of 1971[6].However none of these directly nor indirectly referred to cyber terrorism. For the first time, the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation adopted in Beijing[7]in Article 1 d) provides that an offence is committed when a person destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight. This undoubtedly refers, inter alia to cyber terrorism, but links the offence exclusively to the safety of aircraft in flight. Article 2a) of the Convention provides that the aircraft is considered to be in flight at any time from the moment when all its external doors are closed following embarkation until the moment when any such door is opened for disembarkation; in

[5]Collin, Barry C., "The Future of CyberTerrorism: Where the Physical and Vir- tual Worlds Converge", Remarks at the 11th Annual International Symposium on Criminal Justice Issues

[6]Abeyratne (1998), which discusses extensively the treaties. See also, Abeyratne (2010) at 205–264.

[7]Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, done at Beijing on 10 September 2010.

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

the case of a forced landing, the flight would be deemed to continue until the competent authorities take over the responsibility for the aircraft and for persons and property on board. If therefore as a result of an act of cyber terrorism, a taxiing aircraft collides with an aircraft which has opened its doors for disembarkation but the passengers are still on board awaiting disembarkation, that act would not be considered an offence in terms of the passengers in the process of disembarkation. In other words, the offender would not be committing an offence under the Treaty either against the second aircraft or its disembarking passengers. Nonetheless, the Beijing Treaty of 2010 is a step forward in the right direction with the threat of cyber terrorism looming, affecting the peace of nations. Air transport could well be a target towards the erosion of that peace.

On a more general basis, and certainly of relevance to aviation, are the efforts of various international organizations such as the United Nations, Council of Europe, Interpol, and OECD[8]dating back to the 1980s in responding to the challenges of cyber crime. One significant result of this collective effort was the publication of the United Nations Manual on Cybercrime[9]and United Nations Resolution of 2001[10] which exhorted States, in the context of an earlier UN Resolution on Millennium Goals[11]which recognized that the benefits of new technologies, especially information and communication technologies are available to all—to ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies; while also ensuring law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies which should be coordinated among all concerned States. The Resolution went on to require that information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies and that law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies.

The Resolution recognized that legal systems should protect the confidenti- ality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized and that such systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations. It called upon mutual assistance regimes to ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such

[8]The mission of the Organisation for Economic Co-operation and Development (OECD) is to promote policies that will improve the economic and social well-being of people around the world. OECD provides a forum in which governments can work together to share experiences and seek solutions to common problems. We work with governments to understand what drives economic, social and environmental change.

[9]United Nations Manual on the Prevention and Control of Computer Related Crime, International Review of Criminal Policy nos. 43 and 44 (1999).

[10]United Nations Resolution on Combating the Criminal Misuse of Information Technologies GA RES 55/63, UNGA 55th Session, 81st Plenary Meeting UN Doc. A/RES/55/63 (2001).

[11]A/RES/55/2.

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

cases. States were requested to make the general public aware of the need to prevent and combat the criminal misuse of information technologies. A significant clause in the Resolution called for information technologies to be designed to help prevent and detect criminal misuse, trace criminals and collect evidence to the extent practicable, recognizing that the fight against the criminal misuse of information technologies required the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of governments to fight such criminal misuse.

A seminal event in the international response to cybercrime occurred in 2001 with the adoption of the Cybercrime Convention[12]of the Council of Europe which was opened for signature in November 2001 and came into force on 1 July 2004. The Convention was ratified by President Bush on 22 September 2006 and entered into force for the United States on 1 January 2007. The main concern of the Convention was the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks. States Parties to the Convention therefore expressed their view—in a Preambular Clause to the Convention—that co-operation between States and private industry in combating cybercrime was necessary and that there was a need to protect legitimate interests in the use and development of information technologies. The intent of the Convention can therefore be subsumed under three premises:

(a) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;

(b) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; and

(c) setting up a fast and effective regime of international co-operation.

The Convention in Article 2 requires each Party to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, access to the whole or any part of a computer systemwithout right. The provision goes on to say that a Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or with other dishonest intent, or in relation to a computer system that is connected to another computer system. There are also provisions which call for States Parties to adopt legislative or other measures to counter illegal inception of transmission of computer data, data

[12]European Treaty Series no. 185. Forty two European States, the United States, Canada and many other countries were signatories to the Convention.

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

interception and exchange interception.[13]Of particular significance to aviation is Article 7 on alteration of data and forgery, which goes on to require each Party to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. The Provision concludes that a Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 7 protects certain measures adopted by the aviation community to ensure that the integrity of passports and other machine readable travel documents are protected with technology such as the Public Key Directory (PKD). PKD is based on a brand new technique known as quantum cryptography which is calculated to eliminate the terrifying vulnerabilities that arise in the way digitally stored data are exposed to fraudulent use. This new technique uses polarized photons instead of electronic signals to transmit information along cables. Photons are tiny particles of light that are so sensitive that when intercepted, they immediately become corrupted. This renders the message unintelligible and alerts both the sender and recipient to the fraudulent or spying attempt. The use of a technique such as the public key directory in passports is a good example. The public key directory is designed and proposed to be used by customs and immigration authorities who check biometric details in an electronic passport, and is based on cryptography which is already a viable tool being actively considered by the aviation community as a fail-safe method for ensuring the accuracy and integrity of passport information.

The use of biometric information for the identification of persons is another method that counters cyber terrorism and interference of computer imagery. Biometrics target the distinguishing physiological or behavioral traits of the individual by measuring them and placing them in an automated repository such as machine encoded representations created by computer software algorithms that could make comparisons with the actual features. Physiological biometrics that have been found to successfully accommodate this scientific process are facial recognition, fingerprinting and iris-recognition as being the most appropriate. The biometric identification process is fourfold: firstly involving the capture or acquisition of the biometric sample; secondly extracting or converting the raw biometric sample obtained into an intermediateform; and thirdly creating templates of the intermediate data is converted into a template for storage; and finally is the comparison stage where the information offered by the travel document with that which is stored in the reference template.

NATIONAL EFFORTS

Interception of data is a critically offensive act which serves as a precursor to cyber

[13]Cybercrimes Convention, Articles 3, 4 and 5 respectively.

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

crime and cyber terrorism. The Cybercrime Convention defines interception as:

Listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices[14].

Surveillance laws against interception in the United States have been somewhat ambivalent until they underwent reform in 1986 with the Electronic Communica- tions Privacy Act (ECPA) which was adopted prior to the introduction of the internet and the World Wide Web. Courts have referred to such laws as convoluted[15]and confusing and uncertain. In the decision of Konop v Hawaian Airlines[16],handed down by the United States Court of Appeal 9th Circuit in 2002, the Court noted inter alia that the ECPA defines "electronic communication" as a "transfer" of signals, and that unlike the definition of 'wire communication,' the definition of 'electronic communication' does not include electronic storage of such communications", which drew the Court to the conclusion that the Act was not equipped to handle modern forms of electronic communication[17].

In the United Kingdom, the Regulation of Investigatory Powers Act (RIPA) of 2000 was a legislative attempt by Parliament to unify in a single legal framework provisions responding to the interception of information and communications. RIPA does not discriminate between types of communications or the location at which communications are intercepted. Initially, in Section 1.1. RIPA provides that it is an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a public postal service or a public telecommunication system. In Section 1.1.2. RIPA prescribes it an offence for a person to intentionally and without lawful authority, intercept at any location in the United Kingdom any communication while it is being transmitted via a public or private

telecommunications system. An important provision is Section 4.1. which makes conduct by the interceptor lawful if the interception of a communication in the course of its transmission by means of a telecommunication system constitutes interception carried out for the purpose of obtaining information about the communications of a person who, or who the interceptor has reasonable grounds for believing, is in a country or territory outside the United Kingdom. Such interception would relate to the use of a telecommunications service provided to persons in that country or territory which is either a public telecommunications service; or a telecommunications service that would be a public telecommuni- cations service if the persons to whom it is offered or provided are members of the public in a part of the United Kingdom.

[14]Cybercrimes Convention Explanatory Report, paragraph 53.
[15]US. V. Smith 155 F 3d 1051 at 1055 (9th Cir. 1998)
[16]302 F 3d 868.
[17]Id. 461

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

Australia has adopted the Telecommunications (Interception and Access) Act of 1979 Section 7(1) of which provides that a person must not intercept, authorize, suffer or permit another person to intercept or do any act, or thing that will enable him or her or another person to intercept a communication passing over a telecommunications system[18].A Key provision is Section 108 (1) which provides that a person commits an offence if that person, with intent and knowledge accesses a stored communication or authorises, suffers or permits another person to accesses a stored communication or does any act or thing that will enable the person or another person to access a stored communication where the intended recipient of the stored communication or the person who sent the stored communication had no knowledge of the offender's act.

In Canada a ambivalent legislative structure dealing with unlawful interception of documents and communications. In the absence of specific legislation one could draw parallels in Canada's criminal legislation, for example in the Canadian Criminal Code where Section 184(1) provides that an agent of the Statemay intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication if either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; or the agent of the state believes on reasonable grounds that there is a risk of bodily harm to the person who consented to the interception and he purpose of the interception is to prevent the bodily harm. The provision goes on to require the agent of the State who intercepts a private communication to, as soon as is practicable in the circumstances, destroy any recording of the private communication that is obtained from an interception, any full or partial transcript of the recording and any notes made by that agent of the private communication, if nothing in the private communication suggests that bodily harm, attempted bodily harm or threatened bodily harm has occurred or is likely to occur. It is also important to note that Section 287(1)(b) provides that every one commits theft who fraudulently, maliciously, or without colour of right uses any telecommunication facility or obtains any telecommunication service[19].

POLICY IMPLICATIONS

In terms of a theoretical discussion, any country concerned about cyberterrorism should embrace the double approach. That is, while taking every necessary step to ensure the safety of their critical infrastructures, they should also make every effort to achieve an inclusive partnership/alliance with other countries.

[18]The Act defines a telecommunications system as a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radio communication.

[19]Section 287 defines telecommunication" as "any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio, visual, electronic or other electromagnetic system

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

To achieve such an overwhelming task, different venues should be sought after, including formal and informal cooperation. Cooperation may involve both formal and informal relationships, and the effectiveness of both may vary depending on the case in question. While the desired relationship should be formal cooperation, it has drawbacks, most notably, bureaucratic procedures takes a long time which could be crucial for law enforcement and other national security agencies. Particularly, investigating cyberterrorism does not provide the luxury of spending time for going through bureaucracy. On the other hand, while informal mechanisms are efficient in terms of time, in some countries, informal cooperation may not be approved by their governments. Therefore, in responding to cyberterrorism or cybercrime, both informal and formal cooperation should be put into practice while efforts are being made to lessen the bureaucratic procedures which can be achieved by bilateral agreements.

Awareness is another cornerstone toward achieving real-concrete cooperation. Developing awareness at the domestic and international level toward cyberterrorism and cybercrime will help concerned parties to work with other countries. Recognizing existing or potential risks will motivate countries to start to take necessary measures to respond to cyberterrorism and cybercrime, to include legal, technical, and political procedures.

Another important issue with respect to policy implications is the legal discrepancies and/or lack of legal measures targeting cyberterrorism and cybercrime. While countries amend new laws or update the existing ones to compensate the gap stemming from new trends to respond to cyberterrorism, they also should try to establish a consensus as to what cyberterrorism constitutes and what the general procedures should be in terms of handling investigations and prosecution of cyberterrorism related incidents. Conventions, such as the Council of Europe Convention on Cybercrime –even though there are some questions about the article in the Convention Treaty- is an ambitious attempt toward achieving such a consensus.

In terms of facilitation of cooperation at the national and international levels a number of entities can play important roles. In particular, institutions, such as CERT and FIRST can be instrumental in carrying out informal and formal bilateral and multilateral cooperation. In the area of cyberterrorism and cybercrime such an activity at the informal level among private or public institutions can lead to formal cooperation since informal processes can guide the development of a culture of cooperation. Moreover, entities, such as G-8 and OECD can lead other non-member countries toward developing a certain level of awareness. While these entities do not have operational branches, they can set the standards for future applications and strategies for themselves and be examples for other countries. On the other hand, institutions, such as the UN and the Council of Europe can be more active organizations since they constitute more member states. Also the members can be obliged to fulfill

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

the requests from these multilateral entities, which can be vital to achieve consensus[20].

Also, developed countries can offer technical and legal assistance to other countries; in other words, developed countries can expand the response policies by supporting other countries. One way to accomplish a sound cooperation is to identify regions and focus those areas. Countries such as Turkey can be a center in the Middle East, including the former Soviet Union Republics. Turkey can work with experts from the US and other European countries to train law enforcement in the region in the area of terrorism and cybercrime. Given the fact that Turkey has a long history of struggle against terrorism and organized crime, the experience can be utilized toward advancing regional countries' abilities and understanding toward how to handle terrorism, in particular, cyberterrorism and cybercrime.

Other critical and rather sensitive issues are national sovereignty and jurisdiction. National sovereignty is a political issue that may be an obstacle since countries have every right to claim their sovereignty when it comes to investigating cyberterrorism. Respectively, the issue of jurisdiction becomes a legal issue when investigating cyberterrorism and cybercrime, both of which are transnational in nature. To overcome these two critical issues existing applications from other areas can be considered. Aviation is one of those areas that involve internationally recognized and implemented regulations worldwide. Agreement over such an area can be a model for cyberterrorism and cybercrime initiatives. Another application is the "European Arrest Warrant" which can give a clue as to how the international community will overcome issues of jurisdiction. Of course the author of this study does not imply that we need to have such a system; however, the European Arrest Warrant can be taken as an example.

In terms of overlaps between cybercrime techniques and cyberterrorism, the study suggests that cybercrime techniques are readily available tools for terrorists to exploit. More importantly, technology provides ample opportunity for terrorists to expand their operations and establish new networks with other terrorist organizations. More importantly, cyberspace gives terrorists new tools to recruit new members and to support their activities financially. The C-F-R-P factor is very critical in terms of responding not only to cyberterrorism, but also to traditional terrorism. The C-F-R-P factor can, in fact, be monitored by law enforcement and can be used to identify possible recruitment techniques, possible new recruits, and finance sources. Also, it can provide invaluable information in terms of communication. It is true that not every terrorist organization uses the Internet for communication; nevertheless, communication on the Internet can provide leads for further investigations[21].

[20]Marotta, E. (2001). Europol's Role in anti-terrorism policing. In M. Taylor & J. Horgan (Eds.), The future of terrorism (pp. 14-18). London, England: Frank Cass & Co. Ltd.

[21]Nosworthy, J. D. (2000). Implementing information security in the 21st century- Do you have the

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

CONCLUSION

Cyber terrorism knows no borders. Responding to cyber terrorism requires special efforts, developing strategies and policies and includes bringing efforts from all parties; governments, private sector, and multinational agencies and also requires all concerned parties work together at all fronts, technically, legally, politically, and culturally. These efforts may involve developing new tactics and strategies for effective terrorism response, creating legislation and establishing bilateral and multilateral cooperation taking into account universally accepted principles of law and justice. While taking necessary measures, governments should also be aware that the fundamental rights of individuals should be protected from. There is always tension between protecting the rights of a person and enforcing laws. Fundamental rights, democracy and the rule of law need to be protected in cyber space.

*****

balancing factors? Computer & Security, 19, 337-347.