UTILIZATION OF CYBERSPACE BY TERRORIST GROUPS AND THE APPLICABILITY OF THE MALAYSIAN LAW ON TERRORISM

Mohamad Fateh Labanieh,*[1] Dr. Sonny Zulhuda[2]

[1] Ahmad Ibrahim Kulliyyah (Faculty) of Laws (AIKOL), International Islamic University Malaysia (IIUM), P.O. Box 10, 50728 Kuala Lumpur, Malaysia. Email: fateh.labanie@gamil.com
[2] Asst. Professor, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, P.O. Box 10, 50728 Kuala Lumpur, Malaysia. Email: sonny@iium.edu.my

Keywords:
Cyber terrorism; ISIS; Islamic State; Iraq; Syria; Terrorist groups; SOSMA;

ABSTRACT

It is an obvious and undeniable fact, that the cyberspace is become a powerful method which is increasingly and quickly utilized by terrorist organizations to achieve their gruesome and nefarious goals by hitting innocent individuals. This paper has conducted a critical and comprehensive study on the literature review aiming to answer several inquiries about utilization of cyberspace by terrorist groups and the applicability of the Malaysian law on terrorism. The meaning, characteristics and goals of cyber terrorism will be highlighted. Furthermore, this paper will clarify how terrorist groups invade the cyberspace with highlighting on “ISIS” as an example. In addition, this paper will indicate how the Malaysian Law addresses the terrorism. This paper has proved that the terrorist groups become more sophisticated and complex by adopting the cyberspace. Moreover, this paper discloses how terrorist groups exploit the cyberspace. Even if, Malaysian law adopts many measures and precautions to counter terrorism, but, it still needs more efforts to deal with terrorism, by regulating the “Bitcoins”, introducing a clear definition about the meaning of "lethal device” to encompass harm programs and viruses, and distinguishing between clicking

To Cite This Article: Mohamad Fateh Labanieh and Dr. Sonny Zulhuda. Utilization of Cyberspace by Terrorist Groups and the Applicability of the Malaysian Law on Terrorism. Journal of Asian and African Social Science and Humanities, 2(2): 31-54, 2016

“like” or sharing the terrorist items with use explicit words to glorify the terrorism and without use any explicit glorification words. The lawgiver must take into consideration the possession of terrorist items or publications for academic and innocent purposes. Finally, under SOSMA, the power to intercept the communications must be subjected on the judicial oversight and the power of arrest must be based on objective test.

INTRODUCTION

The emergence of any modern technology brings negative and positive problems. Cyberspace is not different in that regard. It is undeniable reality that the use of cyberspace is now part and parcel of our lives, we cannot dare to imagine life without cyberspace. However, with all its positive contributions in our lives, cyberspace becomes one of the major sources assists to destruct the societies and civilization. This is due to the fact that cyberspace now is considered an easy and effective instrument which has been utilized by the terrorist groups for carrying out their activities.

Use the cyberspace by terrorist groups is an essential transition point from traditional terrorism depends on materialistic means to the modern terrorism relies more on sophisticated and invisible technologies (Furnell, S. M., 1999). In 1980, the cyber terrorism is still theoretical without any perceptible examples. In 1990, the concern of cyber terrorisms increases extensively, and the media concentrates directly on these dangerous issue, the first emergence of cyber terrorisms was in 1998, on Sri Lankan when a group called "Ethnic Tamil Tigers" used cyberspace to attack government websites in order to disrupt and destroy them (Shandra, 2012). In 2007, hackers from Russia launched a cyber-attack to destroy the Estonian government’s websites (Furnell, S. M., 1999).

However, in the present time, the cyber terrorism has continued to be more precise and sophisticated because the extremist groups exploit the significant features which are presented by the cyberspace, enable terrorist groups to communicate easily with each other, via cyberspace without any limitations and the leaders and members of these organizations can disseminate their ideologies and radical views to the large numbers of audiences. In addition, cyberspace further assists the terrorist organizations in terms of coordination and planning. Therefore, cyberspace offers not only considerable benefits and advantages to the terrorist organizations but also it creates plenty of challenges and obstacles in front of states for fighting terrorism. (EwËnÉs Ñarab, 2010). As a result, in this research, we will explain the meaning of cyber terrorisms. In addition, the characteristics and goals of cyber terrorism will be highlighted. Furthermore, the paper will discuss how the terrorist groups invade the cyberspace with giving real examples from the Islamic state (ISIS). Finally, this paper will indicate how the Malaysian law addresses the terrorism.

The meaning of cyber terrorisms

Cyber-terrorism is defined by the Center for Strategic and International Studies (CSIS) defined cyber-terrorism as "*the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population*." (Lewis, J. A, 2002). Another definition of Cyber-terrorism *"is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."* (Kennedy,P , C., Clubb, G., & Mabon, S, 2015).

The characteristic of cyber terrorism

1-Cyber terrorism is considered as a new kind of modern war (SafÊr, × 2013). It happens in a quiet environment without use any physical weapons because the attackers carry out their missions behind the screen of computers without disclosure their identity. In addition, it is done without use any kind of force because cyber terrorism relies on a computers with necessary programs.

2- Cyber terrorism is very cheap compared with traditional terrorism which imposes on the members to purchase lethal explosives and expensive materials (Goodman, J, C. Kirk, Megan H. Kirk, 2007). In contrast, cyber terrorism is launched by use cheap materials (computer).

3- Cyber terrorism is very easy, it does not require the same degree of efforts which require for achieving the purposes of the traditional terrorism (N. Veerasamy, 2009), because cyber terrorism can be established by individuals who are expert in utilizing the internet and the computer systems.

4- Cyber terrorism is a trans-border terrorist crime towards the countries because the attackers can target any state from their places without having to incur the trouble to travel to the location of target. So, it is done either from the same place where the target is located or from different places.
5- The difficulty in proving the cyber terrorism (ÑaÏeah, 'aesar, 2014), because it does not leave any physical evidence, as will the evidence can be easily removed.

The goals of cyber terrorism

1- To spread the fear and terror among the individuals in different countries by attack the main computer systems which control the vital infrastructures in order to obstruct their works such as electricity transmission networks and nuclear power factories (BawaÉdy, 2006).

2- Exposing the integrity and security of society on the risk by disturbing public order (ÑaÏeah, 'aesar, 2014). For example, destroying the vital infrastructures such as oil refineries or bank computer systems.

Why the terrorist groups use the cyberspace

Propaganda
According to "Ayman al-Zawahiri" who is present head of al-Qaeda, says that *"al-Qaeda is in a battle, and more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our people"* (Barakat, I, 2014). The primary goal for use the cyberspace by terrorist groups is to disseminate the propaganda globally. In general, the propaganda takes plenty of forms such as audios or videos.

These forms assist the terrorist organizations to provide not only to their ideological orders but also, to promote their activities in a wide scale (Awan, I, 2014). Also video games which are developed by the terrorist organizations are played an integral part in disseminating a terrorist propaganda, in 2014, "ISIS" had launched an android application called *"Dawn of Glad Tidings"* The main function of this application is to provide users with breaking news about ISIS activities, its suicide operations and its victories in the battlefield (Siboni, G., Cohen, D,. and Koren, T, 2015). However, luckily, "Google play store" removes this application from its store (FoxNews, 2014).

Furthermore, ISIS seeks to revive its dogma represented in the idea of electronic jihad which aims to spread negative propaganda. So, ISIS creates not only media organizations such as the Dabiq foundation (CBC News, 2015), but also radio station such as “Al Bayan" (Hayward, J, 2015). As a result, the authors think that the terrorist organizations not only strive to control the cyberspace as much as possible but also create an illusion among people and attract them to participate with them.

Recruitment

Cyberspace has been utilized by terrorist organizations as a systematic method for controlling the weak minds and recruiting new fighters. Various online platforms have been employed progressively by the terrorist groups in order to achieve this purpose such as chat room or social media (Eshpar, Y., Baram, G., Averbuch, A., Siboni, G., Cohen, D., Rotbart, A., Crosston. 2013).

Therefore, the propaganda has been designed by the terrorist organizations with concentrating on the social and economic situation of victims in order to exploit these sentiments as a weapon for recruiting such as sentiments of humiliation, injustice and exclusion (Minei, E., & Matusitz, J., 2012). So, in this point, the authors think that the terrorist propaganda attempts as much as possible to target the marginalized groups by preparing a detailed investigation about the victim in order to know clearly the right way to dominate him and plant a poison inside his mind.
Such one example is, “al-Furqan Institute” and “al-Hayat” have been created by ISIS for recruiting huge numbers of individuals by releasing speeches and video clips which had translated for more than one langause (Crethiplethi, 2014). In addition, the online video games can be used significantly as a method of recruitment (Weimann, G, 2014). With respect to what we have discussed earlier, the authors believe that ISIS for example adopts systematic and sophisticated tactics for controlling minds and recruiting the international fighters, compared with traditional terrorist organizations because ISIS employs more than one language in its media for recruiting.

Incitement and Psychological Warfare

Generally, propaganda is not prohibited in all countries around the world but employment the propaganda by terrorist groups for incitement to commit violence is considered as an unlawful act. Internet has been used widely and significantly by the terrorist groups for the purposes of incitement. Such one example is in 2016, the propaganda machine does not stop at all for incitement the individuals around the world to carry out suicide operations and terrorist operations in other countries. Because the “Wa’ad media institution” which supports ISIS, had released new video called *“Fight them, Allah will punish them by your hands”* this video encourages the terrorist fighters to launch suicide attacks in London, Berlin and Rome (Dearden. L, 2016).

Moreover, cyberspace plays a fundamental role in use the psychological warfare by spreading horrific videos and images among the individuals around the world (Weimann, G, 2004).

For instance, on Mosul in June 10, 2014, ISIS depends on social media to spread fear on a large scope by targeting the hearts of individuals. Therefore, ISIS has issued a horrific video depicts the operation of decapitations, this video is part of the systematic media campaigns to ingrain dread and horrified feelings in the hearts of Iraqi citizens in order to show them what "ISIS" will do if the Iraqi citizens show any kind of resistances (QÉÍtaÉnyÊ, M., QÉÍtaÉnyÊ, M, 2014). In addition, ISIS adopts modern method by use twitter platformm this method called “hashtag” seeks to put pressure on a particular government to succumb to its demands. For instance, when ISIS kidnaps an American journalist in Syria, ISIS uses the hachtag of “*StevensHeadInObamasHands*” in order to pressurize on President Obama to stop the military operations in Syria (Trowbridge, A, 2014).

Financing

According to the terrorist organizations *“Money is considered as not only terrorism’s lifeline but also money is the engine of the armed struggle”* (Conway, M, 2006). Traditionally, the most significant problem which faces the terrorist organizations is represented in the issue of financial transactions and support. But, in this decade, the ways which are used by terrorist organizations to handle these kind of problems, have been totally changed.

Therefore, the terrorist groups adopt a lot of advanced methods in order to collect money for support their extremist activities (Brantly, A, 2014). Such as, utilizing the online stores offer motivational jihadist materials such as songs, videos, E-books, and various items (Conway, M, 2006). Or by use the dark web *“is a collection of thousands of websites that use anonymity tools which help the terrorist organizations in hide their IP address and protect users from surveillance and censorship* (Greenberg, A, 2014). Such one example is, ISIS has collected money by accessing to the “DarkWeb” and exercising the illicit trades such as oil, antiquities, and human trafficking (Bertrand, N, 2015).

Just for highlighting, there is an assuming that ISIS may support its activities by use an advance way which called “Bitcoin” *“is virtual currency, uses through the internet, it is not backed by any country's central bank or government”* (Rouse, M, 2013). Because, in 2015, there is secret document had released from a person who supported ISIS, the title of this document was called *“Bitcoin and the Jihad handout”,* the document was written by “TÉqÊy al-DÊyn al-Mundhir”, this document encouraged the members of ISIS to use the Bitcoin for finance their activities and for the purpose of money laundering in a safe way without any tracking by the governments, also this document explained how the jihadists can use the Bitcoin in an authoritative way (Al Bar qËw qÊy, M, 2015).

As a result, the authors believe that if the terrorist organizations like “ISIS” will use the Bitcoins in the future that will be a very strong “weapon” because this method will give them capabilities to support their missions outside the financial government records. So, it is suggested that the Malaysian governments should intervene quickly in order to regulate the “Bitcoins” and take a security measures.

Furthermore, one of the modern method which is adopted dramatically, is called the “Hawala network” as *“an alternative or parallel remittance system”* (Patrick M. Jost, Harjit Singh Sandhu, 2003), this system not only is existed and operated outside the governmental control but also, it is based on communication systems such as phone, fax, or email among either the members of Hawala dealers or the members of Hawaladars (Drifter, 2004). For example, al Qaeda utilized the Hawala system prior its attack against the United States in 11 September 2000 by transferring huge amount of money to different accounts (Faith, D, 2011). The authors in this point argue that “Hawala network” has been adopted by the terrorist organizations significantly due to its important features such as the difficulty of tracking or monitoring by the competent authorities as well this system is very cheap and trusted. So, it is suggested that the competent authorities must take preventive measures to monitor and control this method.

In addition, regardless of the modern methods, the terrorist organizations have a bad history in exploiting charities as a method of fundraising (Baron, B. F., 2004). They employ charities which appear like legitimate organizations with legitimate purposes such as collecting funds for humanitarian purposes “the Syrian case” but in reality, these charities will strive to achieve illicit purposes. Such one example is, Shafi al-Ajmi who is arrested by a Kuwaiti government, because he collected funds for ISIS under the name of charitable acts (Janine Di, Leah, and Damien, 2014).In this case, the authors believe that the individuals must be more aware and attentive because terrorist organizations attempt to take advantage from the obligations of Muslims towards Allah in terms of giving donations.

Planning, intelligence, coordinating and training

Cyberspace is employed by terrorist organizations for planning to launch terrorist operations and intelligence purposes. Commonly, it is used to identify and obtain significant information about the best ways for attacking the targets (Edelman, J, 2014). For instance, a man had been arrested by the Australian authorities because he utilized Web sites related to the Australian government in order to collect information (maps and data) about the potential targets (Theohary, C, A, 2011). Or by use the applications such as "Google map" which provides sufficient and detailed data about the location of potential targets (Harding, T, 2007). In addition, through social media such as Twitter, Facebook and LinkedIn, the terrorist organizations can gather a personal and unique information about the person who will be targeted by them in the future (Ñarab, Y, 2010).

As well as, cyberspace plays an essential role in coordinating between the terrorist members, for instance, in 2015 after Paris attack, that killed 129 people and wounded more than 100, there is a supposition that the members of ISIS had used a device called "play station 4" and through the online game called "call of duty" they planned and coordinated to their suicide attak without writing or uttering any single word because ISIS's members communicate with each others by shooting the bullets at the wall for writing their massages (Halkon, R, 2015).

Generally, terrorist groups and particulary ISIS are adopted videos games as a method for training and preparing the new jihadists to the battlefield, such one example is a game called "Jihad Simulator" offers information about the mechanism of building bomb and how the jihadists can drive truck in easy way (Gabi, S., Daniel, Cohen. & Rotbart, A, 2015). Moreover, in the cyberspace there are a lot of jihadist websites which provide videos, audios and E-magazine with more than one language teach the Jihadists how they can launch suicide attacks cause a large number of casualties and how they can encrypt their communications (Andrew, J, A., 2002).

From this perspective, the authors believe that the path of terrorism has become very easy, because the important features which are offered by the cyberspace, facilitate the terrorist operations. So, the authors argue that the international governments in general and the Malaysian government particularly must take bold steps in order to monitor and stop use the cyberspace by the terrorist groups for achieving terrorist activities.

Cyberattack

Previously, the terrorist organisations do not have enough cappabilities and resources to launch cyberattack but in recent years, the threat of terrorist organizations has increased dramatically. this threat starts to be real after issuing a report assumes that "ISIS" had moved to the next stage of terrorism by adopting the cyberspace which will give ISIS the ablilities to launch cyber-attack on the vital infrastructures such as air ports, train staions and other vital companies (QÉÍtaÉnyÊ, M., QÉÍtaÉnyÊ, M, 2014). As well as, according to ISIS, cyber-attack brings significant results are embodied by damaging the vital infrastructures of the states, modifying or removing the important data and preventing the authorized users to access to their personal information (WazaÉrt Al 'wqaÉf Al SwËrehÊ, 2014).

Even if, there are a lot of examples about cyber-attacks are done by ISIS, but these attacks still classified as weak attacks because the lack of experiences. Such one example is, ISIS creates a group called “Cyber Caliphate”, it considered as a right hand for ISIS in the cyberspace, this group attacks the Malaysia Airlines website and disseminates ridiculous phrases such as *“ISIS will prevail ”, “404-Plane not found”* (Hill, G., 2015). In 2015, YouTube and Twitter accounts of the the Central Command of the US Army are hacked by the ISIS "cyber-jihadists" which stealing confidential information such as email addresses and phone numbers of the employees at the American military (Lamothe, D., 2015).
The authors consider that according to the worldwide opinion, ISIS is similar than a black plague in terms of a degree of hazard and lethality. So, it is suggested that the governments around the world must cooperate with each other in order to protect their infrastructures because the terrorist organizations in the future will not only fight without firing any bullet but also will strive to attack vital targets rather than weak targets by recruiting and hiring the specialist individuals in computer systems. In addition, because cyber-attack achieves the goals of the terrorist groups with less cost.

HOW MALAYSIAN LAW ADDRESSES THE TERRORISM

Protecting public safety is considered as an initial priority in the Malaysia’s transformation agenda for becoming a superior nation. Therefore, the Malaysian government has being made formidable endeavors which are embodied not only to protect the public safety but also to prevent any danger or harm on its public (Simon, W, 2014). So, anything which can be made by the competent authority in order to stop the hazards on the public can be considered as a useful action for guaranteeing the protection of the public safety.

As a result, in order to achieve this purpose, Malaysian government starts with the “ISA” (The Internal Security Act 1960) contains a lot of imperfections compared with its advantages, in 2012, “ISA” was abolished by applying “SOSMA” the “Special Offences (Special Measures) Act”
The main significance in “SOSMA”, is that the minister has no more authority to detain the persons because this power has been moved to the court in order to ensure that this power will be applied in a fair way without arbitrary practices from the side of the executive authorities (Dhanapal, S., Sabaruddin, J. S., 2015).

Regardless of “SOSMA”, the Malaysian government has issued a crucial and new amendment of the Malaysian Penal Code 574 which deals with the increased threats against the nation security (public safety), comprises two chapters, the first chapter VI (offences against the State) starts from sections 121 to 130A, the second chapter VIA (Offences relating to terrorism) starts from sections 130B to 130T.

So, this part will focus on the procedural part of detention under (SOSMA). As well as, the substantive part of penal code 574 will be discussed critically by selecting the related articles which are applied by the Malaysian authority for fighting the terrorism and prevent exploiting the cyberspace by the terrorist groups.

The procedural part (SOSMA)

SOSMA has been divided into eight parts. But as we mentioned previously the authors will select the related articles in order to give an overview about the arresting mechanism under this law. Initially part I, section (2) stipulates that SOSMA shall be applied to any security offences which are mentioned in VI (offences against the State) and VIA (Offences relating to terrorism) of the Penal Code 574. According to (S/4) a police officer has a right to detain or arrest a suspect if a police officer has a reason to believe that this person is involved in any security offences. However, for the purpose of investigation, the period of arresting is only for 24 hours (S4/4) but this period can be extended until 28 days by the police officer or above the rank of superintendent (Section 4/5).

According to the authors, the state must have a wide and strong powers in order to face the "Black danger" represented in terrorism and protect not only its security but also its integrity. However, the authors criticize that the power to arrest is based on subjective test rather than objective test because the arrest under SOSMA needs only the reason from the side of the police officer to think that the person is implicated in any kinds of security offences without any physical evidence. So, it is suggested that the detention must be based on objective test in order to ensure that this law will not be applied as a tool of oppression and infringement the rights of citizens.

In addition, the police officer has an opportunity to decide whether the detention is necessary or not, but if the police officer decides that the detention is not necessary, the suspect will be released after attaching the electronic monitoring device on him. (S4/6) In contrast, if the police officer or above the rank of superintendent has decided to remain the suspect in detention for up to 28 days, this detention must be reconsidered every five years unless a resolution is passed by both Houses of Parliament in order to extend the period of operation of the provision. (S4/11). (S5/1/A) and (S5/1/B) stipulate that When an individual is detained by police man, the police man must immediately inform his relatives "the next-of-kin" about the issue of detention, as well the suspect still has a right to consult not only a legal practitioner but also he has a right to select legal practitioner. The authors argue in this point that this article aims to protect the public safety rather than suppression the people because the suspect still has a power to exercise his rights. Furthermore, the police officer must inform the suspect as soon as possible about the reasons of arrest (S 4/2).

The police officer has ability to intercept the communications of the suspect for the purpose of investigation, if the police officer thinks that these communications will contain any kind of information which relate to the commission of a security offence (Article II/S6). The Public Prosecutor has authority to require from the communications service provider to retain a particular communication, intercept a communication, and require from the police officer to enter the premises and install a device on the premises for assisting him to gather important information only if the Public Prosecutor has thought that these communications will include any kind of information relating to the commission of a security offence (S6/2).

In this point, the authors believe that the power to intercept the communication must be subjected on the judicial oversight because the public prosecutor who believes that the interception is likely to include information relating to a security offence, can use his authority arbitrarily for interception without obtaining any permission from a judicial officer. So, the authors think that the competent authorities must seek to achieve equilibrium between respecting the privacy and protecting the public interest. So it is suggested that the interception of communication must be under the judicial oversight.

Moreover, the authors want to highlight on a hotly debated issue “tensions between safety and privacy" between Apple VS FBI (Calmaur, K, 2016). In accordance with the facts, FBI requires the helping of Apple Company in order to access and decrypt the suspect’s phone *“Syed Rizwan Farook”* who is a one of the shooters in the San Bernardino attacks (Ahmed, S, 2015). It is noted by the authors that this matter may be regarded as the worst dilemma in 21 century. However, the authors strive to build their opinions according to the "public interest" because they believe that there is an urgent necessity for making an equilibrium between the discordant rights protecting the "public interest" and protecting the privacy. The authors consider that this goal may be achieved by giving priority to the public interest over private interest with applying some precautionary measures to make sure that the privacy rights will not be violated repeatedly. As well as, in order to support this opinion, there is a survey which has done by the “Pew Research Centre”, the result of survey indicates that “51%” of respondents support the efforts which require from Apple to give its assisting to the FBI in order to unlock the iPhone. However, "38%" of participants reject this idea and the rest abstained (Leswing, K, 2016).

The court has a right to determine the period of attaching the electronic monitoring device. As well as, this period must not exceed the remainder of the twenty-eight day period from the date of detention (Part III: S7/1). Also, the security offences shall be subjected to the High Court (Part V).
Part VII, (S24) under SOSMA the court can accept the documents which are confiscated not only in the course of an investigation but also during the raid (S20). As well as, (S24, S25) accept the information which is gathered during the interception of communications or any documents produced by the computer. The authors noted that this article is comprehensive because it covers not only the concrete evidence but also the intangible evidence for example the E-document. Finally, according to the authors that "SOSMA" concentrates on both the deterrence and sanctions, and it still needs a few improvement in order to avoid the tyrannical and arbitrary use.

The substantive part (Penal code 574 chapter VIA- Offences relating to terrorism)

In Malaysia, there is no specific law regulates the cyber terrorism. However, according to Chapter VIA Section 130B (3) (H) of Penal code:

> *"An act or threat of action falls within this subsection if it— (h) is designed or intended to disrupt or seriously interfere with, any computer systems or the provision of any services directly related to communications infrastructure, banking or financial services, utilities, transportation or other essential infrastructure"*

So, in chapter VIA Section 130B (3), the Malaysian law determines the acts or threats which amount to be as terrorist acts. However, particularly from the spirit of the article 130B (3) (H) we can see that the Malaysian law is very precise by taking into consideration the acts of cyber-terrorism. Therefore, from what we discussed above, we can conclude that the Malaysian penal code 574 has addressed the act of cyber terrorism.
According to Section 130D:

> "*Providing devices to terrorist groups. Whoever knowingly provides or offers to provide any explosive or other lethal device to (a) a terrorist group;(b) a member of a terrorist group; or (c) any other person for use by, or for the benefit of, or terrorist group or a member of a terrorist group, shall be punished with imprisonment for life or imprisonment for a term not exceeding thirty years, and shall also be liable to fine"*

The Malaysian legislator is inclusive and transparent in terms of considering the acts of supplying explosives or lethal devices to any terrorist member or group or for the benefit terrorist member or group as terrorist acts which amount to be punishable by the law. On the contrary, the authors think that the legislator is not clear because he only covers the explosives and lethal devices without giving any explanation about an important issue related to supply harm programs or viruses or malware in order to launch cyber-terrorism harms or disrupts the vital infrastructure and kills the innocent humans. So, the authors wonder whether the Malware or viruses are covered under this article?, and the authors insist on the necessity that the legislator must give clear definition about the "lethal device" in order to encompass harm programs, viruses and malwares. According to section 130E,

> *"Recruiting persons to be members of terrorist groups or to participate in terrorist acts. Whoever knowingly recruits, or agrees to recruit, another person to be a member of a terrorist group or to participate in the commission of a terrorist act shall be punished with imprisonment for a term which may extend to thirty years, and shall also be liable to fine".*

This article penalizes the act seeks to recruit the individual who becomes a member of terrorist organization or participates in any terrorist act if some conditions are fulfilled, the person is knowingly recruited or he accepts the recruiting. In addition, the authors wonder whether this article can be applied to any kind of recruiting methods such as use the social media networks (Facebook or twitter) or cyberspace. So it is suggested that the Malaysian legislator must take into consideration the importance of this issue. As well as, the Malaysian legislator is right in terms of imposing large punishment to these kind of acts. Because this punishment will play an important role in deterring individuals to commit like these acts.

In case of Public prosecutor V Atik hussin bin abu bakar, the court held that the one of suspects is charged under section 130E and 130K of the Penal Code for recruiting persons to participate of terrorist groups and for hiding persons who are committing terrorist acts. In addition, the five other accused are charged under section 130KA while the rest of them are charged under section 130K read with section 511 of the Penal Code. (Sario, R, 2013) In section 130F:

> *"Providing training and instruction to terrorist groups and persons committing terrrorist acts.Whoever knowingly provides training or instruction, or agrees to provide training or instruction (a) in the making or use of any explosives or other lethal device; (b) in carrying out a terrorist act; or (c) in the practice of military exercises or movements, to a member of a terrorist group or a person engaging in, or preparing to engage in, the commission of a terrorist act shall be punished with imprisonment for a term which may extend to thirty years, and shall also be liable to fine."*

And section 130FA says,

> *"Receiving training and instruction from terrorist groups and persons committing terrorist acts. Whoever receives training or instruction, or agrees or arranges to receive training or instruction (a) in the making or use of any explosive or other lethal device; (b) in carrying out a terrorist act; or (c) in the practice of military exercises or movements, from a member of a terrorist group or a person engaging in, or preparing to engage in, the commission of a terrorist act shall be punished with imprisonment for a term which may extend to thirty years, and shall also be liable to fine"*

In both articles (130F, 130FA), the Malaysian legislator only takes into consideration the issue of providing physical training or giving tangible instructions. However, the authors wonder whether the issue of providing or receiving the training and instructions which are done through the cyberspace, are covered by these articles. Therefore, it is suggested that these articles must be inclusive and clear by covering the matters of providing or receiving the training and instruction by use the cyberspace. Also, the lawgiver should provide a precise definition of the term of "lethal device" in order to include harm program, malware and various. As well as, there is no doubt that the Malaysian legislator is very strict in terms of giving a long punishment which helps in reducing these kind of activities. According to the section 130G provides,

> *"Inciting, promoting or soliciting property for the commission of terrorist acts. Whoever knowingly-- (a) incites or promotes the commission of a terrorist act; (b) incites or promotes membership in a terrorist group; or (c) solicits property for the benefit of a terrorist group or for the commission of a terrorist act, shall be punished with imprisonment for a term which may extend to thirty years, and shall also be liable to fine"*

The lawmaker is very accurate because he seeks to penalize the acts which motivate and incite for commission of terrorist acts. However, the writer think that the Malaysian law is still very shy form highlighting on a significant and hot issue plays a pivotal role in reducing the phenomenon of terrorism. Because this article condones the emotional side which produces a lot of negative effects. According to the authors, the emotional side is considered as the first step in the dark road toward terrorism. So, the authors wonder about the controversial question whether the person who is only clicking "like" button or sharing the terrorist videos or photos in the social media or in cyberspace without showing any kind of glorification to the terrorism or terrorist acts, is his acts will be classified under the acts of inciting, promoting or soliciting for the commission of terrorist acts or not?

Therefore, it is noted that these acts shall not be considered as inciting, promoting or soliciting and glorification of terrorist acts because the Malaysian law must distinguish between the case of direct and explicit support through the explicit words which are used by the person during clicking "like" button or sharing these terrorist videos or photos and the case of clicking "like" button or sharing these terrorist videos or photos without showing any kind of the emotional supports which are embodied through the explicit words of glorification the terrorism.

In case of PP v. Yazid Sufaat, Halimah Hussein and Muhammad Hilim Hasim [2014] 2 CLJ 670, the court held that the Yazid will be charged for promoting an act of terrorism and that act was considered as being intended as a threat to the members of the public in Syria under the Penal Code section 130G (a). And Muhammad Hilmi and Halimah Hussin will be charged for incitement with Yazid. According to section 130J says that,

> *"Soliciting or giving support to terrorist groups or for the commission of terrorist acts. (1) Whoever knowingly and in any manner solicits support for, or gives support to (a) any terrorist group; or (b) the commission of a terrorist act, shall be punished with imprisonment for life or imprisonment for a term not exceeding thirty years, or with fine, and shall also be liable to forfeiture of any property used or intended to be used in connection with the commission of the offence. (2) For the purpose of subsection (1), "support" includes (a) an offer to provide, or the provision of, forged or falsified travel documents to a member of a terrorist group; (b) an offer to provide, or the provision of, a skill or an expertise for the benefit of, at the direction of or in association with a terrorist group; (c) entering or remaining in any country for the benefit of, or at the direction of or in association with a terrorist group (d) becoming a member of a professing membership of a terrorist group; (e) arranging, managing or assisting in arranging or managing a meeting to further the activities of a terrorist group; (f) using or possessing property for the purpose of committing or facilitating the commission of a terrorist act;(g) accumulating, stockpiling or otherwise keeping firearms, explosives, ammunition, poisons or weapons to further the activities of a terrorist group; (h) arranging, managing or assisting in arranging or managing the transportation of persons to further the activities of a terrorist group; (i) travelling to, entering or remaining in any foreign country to further the activities of a terrorist group or to commit a terrorist act;(j) encouraging or inducing any person to leave*

> *Malaysia to further the activities of a terrorist group or to commit a terrorist act; or (k) using social media or any other means to (i) advocate for or to promote a terrorist group, support for a terrorist group or the commission of a terrorist act; or (ii) further or facilitate the activities of a terrorist group".*

The authors argue that the Malaysian legislator sees from the wide angle in terms of soliciting or giving support to terrorist groups or for the commission of terrorist because, regardless of the importance of this article in terms of counter-terrorism, the authors want to highlight particularly on the paragraph (K), this article plays a pivotal and an essential role in deterring either the terrorist members or their sympathizers from use the cyberspace in order to promote for terrorist activities. Furthermore, in this article the Malaysian lawmaker is very inclusive because it covers directly the social media and indirectly the "other means" such as charity foundation and cyberspace. Therefore, it is noted that the lawgiver has used flexible and thorough term instead of restricted and specific terminology in order to ensure covering every means which assist the terrorist organizations for achieving their terrorist purposes.

Four international individuals and one Malaysian citizen are detained because of joining the terrorist group and planning of recruitment the jihadists and sending them to fight beside the ISIS in Syria. As well as, one of the suspects is pledged loyalty via Facebook to the leader of ISIS in Syria (Abu Bakar al-Baghdadi). Therefore, the competent authorities convict them under the Chapter VIA on Act 574 Penal Code and the investigation procedures subject to SOSMA act. (borneo , 2015)
In section 130JB says that,

> *"Possession, etc. of items associated with terrorist groups or terrorist acts. (1) Whoever, (a) has possession, custody or control of; or (b) provides, displays, distributes or sells, any item associated with any terrorist group or the commission of a terrorist act shall be punished with imprisonment for a term not exceeding seven years, or with fine, and shall also be liable to forfeiture of any such item. (2) In this section "item" includes publications, visual recordings, flags, banners, emblems, insignia and any other thing displaying symbols associated with a terrorist group, terrorist act or ideology of a terrorist group; "publications" includes all written, pictorial or printed matter, and everything of a nature similar to written or printed matter, whether or not containing any visible representation, or by its form, shape or in any other manner capable of suggesting words or ideas, or an audio recording and every copy, translation and*

> *reproduction or substantial translation or reproduction in part or in whole thereof".*

This article has shown the desire of the Malaysian legislator to prevent the phenomenon of extremism because in this article he is totally comprehensive in terms of giving an accurate and full definitions for the word "items" and "publications" which include not only the physical publications but also the electronic publications that can be obtained via the Internet by downloading these items such one example is (terrorist logo, video, audio and E-document). However, in terms of possession, the authors wonder whether the lawgiver takes into consideration the intention of the possessor who holds terrorist items. Because there are many situations in which the possessor holds these terrorist items for innocent or academic purposes. It is suggested that this section must be more flexible instead of strict especially for those who hold these items by mistake or for academic purposes.

In case of Mohd zidi Said, the court held that the suspect is guilty because he has a photo of Islamic State's flag of "ISIS" in his phone. So, he is charged under Section 130JB (1/a) (Bernama, 2015).

In case of Ahmad Kamil Ghazali, the court held that according to Section 130 JB (1)(A) of the Penal Code, he is guilty because he has possessed terrorist E-documents which have been downloaded from the internet (Gunaratnam, S., 2016). In section 130O,

> "*Providing services for terrorist purposes.(1) Whoever, directly or indirectly, provides or makes available financial services or facilities (a) intending that the services or facilities be used, or knowing or having reasonable grounds to believe that the services or facilities will be used, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act, or for the purpose of benefiting any person who is committing or facilitating the commission of a terrorist act; or (b) knowing or having reasonable grounds to believe that, in whole or in part, the services or facilities will be used by or will benefit any terrorist, terrorist entity or terrorist group, shall be punished (aa) if the act results in death, with death; and(bb) in any other case, with imprisonment for a term of not less than seven years but not exceeding thirty years, and shall also be liable to fine."*

The Malaysian lawgiver has mentioned explicitly in this article about the direct and indirect providing services which are based on reasonable grounds of suspicion that these services will be used to carry out a terrorist act, would amount to be a punishable offense, such as providing financial support. The authors agree, that the Malaysian lawmaker is seen from a wide angle without any limitations in terms of “providing financial services or facilities" because he also encompasses the providing aid or services from the side of lawyer or accountants acting as nominees or agents for their clients.

CONCLUSION, FINDINGS AND RECOMMENDATIONS

There is no doubt that terrorism has become a major obstacle in front of both the developed and developing countries in terms of ensuring the safety of their citizens. As well as, we can see clearly that the terrorism has entered more advanced and complex stages in contrast Malaysian law still need more efforts in order to fight this serious threat because the precautionary and preventive measures which had been adopted did not achieve the appropriate level of requirements for fighting the terrorism.

This paper finds that the terrorist groups have become an annoying obsession for all states around the world in which they have become an easy target for these groups which can exercise their terrorist activities from anywhere in the world through the internet. In addition, this paper highlights that cyberspace provides not only a lot of features but also the extremist organizations seek deliberately to create websites or pages on the internet as a part of their media campaigns in order to disseminate their harm ideologies and principles.

As well as, this paper finds that the terrorist organizations like “ISIS” utilize the audio-visual technologies widely and cyberspace has been used dramatically by the terrorist groups for many purposes such as intelligence, planning, coordinating, recruitment, inciting, and psychological warfare.

This paper discloses that “ISIS” maybe in the future will not only fight without firing any bullet but also will strive to attack vital targets due to it has enough money and capability to recruit the experts. Also, this paper shows that “ISIS” adopts systematic and sophisticated tactics for controlling minds and recruiting the international fighters compared with traditional methods by employing more than one language in spreading its propaganda.

This paper mentions that the cyberspace has been adopted as a tool by the terrorist groups to fund their activities and collect donation such as use “Dark web”. As well as the “charity foundations have been used in a bad way by the terrorist groups. This paper discovers that “Hawla Network” has been harnessed spectacularly by the terrorist groups due to its significant features such as the difficulty of tracking, monitoring and cheapness. Also, this paper shows specifically that ISIS adopts the same traditional methods which are followed by the other terrorist organizations

for finance operations with highlighting on a strong and dangerous presumption shows that ISIS will use the “Bitcoin” in the future.
As well as, this paper discloses that even if the SOSMA and Penal Code 574 in somehow are totally perfect and comprehensive but from the other angle, they still need more efforts and amendments in order to keep up with the wheel of evolution for dealing with terrorism. This paper indicates not only that the new amendment of penal code 574 has addressed the cyber terrorism but also the power of arrest under SOSMA is based on subjective test as well the interception of communication is done without judicial oversight . Also, this paper highlights that the Malaysian law is still silent in terms of regulating the issue of “Bitcoin”. Also, Section 130F and 130FA take into consideration only the issue of providing physical training or giving tangible instructions rather than providing training and instructions via cyberspace. Section 130E does not mention anything whether the issue of recruiting via cyberspace will be covered or not.

Section 130JB is totally comprehensive in terms of giving an accurate and full definition for the word “items” and “publications” which include the physical publications and electronic publications on the contrary, the lawgiver does not mention anything about the intention of the possessor whether he holds these items or publications for innocent or academic purposes. This paper shows that in section130J (2/K) the lawgiver has utilized elastic and inclusive terminologies such as the “other means” rather than restricted terminologies in order to cover the activities of terrorist groups in both the real and virtual life.

Finally, some recommendations will be introduced by the authors, fighting against the terrorism is considered as a new war requires international cooperation among the countries around the world. The private and public sectors in Malaysia must cooperate widely for fighting this dangerous threat. The Malaysian government must adopt the same “weapons” to counter the modern terrorist groups like "ISIS" by hiring the individuals in this war through imposing an obligation on the individuals to give reports for any terrorist page or website which exists in the cyberspace, offers or promotes any support to the terrorist groups. The Malaysian authorities must take bold steps to monitor and restrict the terrorist activities in the cyberspace.

The Malaysian authority must attempt as much as possible to increase its preventive measures to repel any potential cyber-attack affects negatively on the vital infrastructures. As well as the competent authorities in Malaysia must increase the number of the awareness campaigns in order to educate the citizens how they can protect themselves from falling into the trap of terrorism through activating the role of the mosque and the family which play an essential part not only in warning to the seriousness of terrorism but also in striving to strengthen the religious faith. The individuals must be more aware when they give donations to the charity foundations because the terrorist organizations attempt to exploit the obligations of Muslims toward Allah. Under “SOSMA” the power to intercept the communications must be subjected to the judicial oversight to avoid the arbitrary use.

Moreover, under SOSMA, the power of arrest must be based on an objective test rather than subjective. The Malaysian legislator in the penal code 574 must give clear definition about the "lethal device" in order to encompass the harm programs, viruses, and Malware. Malaysian law must take preventive measures for regulating the “Bitcoins” and monitoring the “Hawala Network”. Also, section 130E must encompass the issue of recruiting by use cyberspace and section 130F and 130FA must be more precise in terms of covering the matters of providing or receiving the training and instruction via cyberspace.

In section 130JB the lawgiver must avoid the generalizing and strictness by taking into consideration the difference between the possession of terrorist items or publications for innocent or academic purposes and for bad purposes. Finally, in section 130J(K), the lawgiver must distinguish between the case of clicking "like" or sharing the terrorist items with use explicit words to glorify the terrorism and the case of clicking "like" or sharing terrorist items without use explicit words to glorify the terrorism.

REFERENCES

Awan, I. (2014). Debating the Term Cyber-terrorism: issues and problems. *Internet Journal of Criminology*. ISSN 2045 6743. Pp. 1-14.

Ahmed, S. (2015). Who were Syed Rizwan Farook and Tashfeen Malik?. *CNN*. <http://edition.cnn.com/2015/12/03/us/syed-farook-tashfeen-malik-mass-shooting-profile>. Accessed on: 25/3/2016

Al Bar qËw qÊy, M. (2015). bÊytkËwen wa al dyÊnal al dhÉhabËy hal yandÉmj daÉÑsh fÊy al mËjtamÑ al dËwaly?. *Masr alarabia*. <http://www.masralarabia.com Accessed on: 27/2/2016

Brantly, A. (2014). Financing terror bit by bit. *Compating terrorism center*. <https://www.ctc.usma.edu/posts/financing-terror-bit-by-bit>. Accessed on: 14/3/2016

Bernama. (2015). Soldier gets 7 months' jail for IS image on mobile phone. *malaysia kini*. <https://www.malaysiakini.com/news/316470>. Accessed on: 4-3- 2016.

Bertrand, N. (2015). ISIS is taking full advantage of the darkest corners of the internet. *Business insider*. <http://www.businessinsider.my/isis-is-using-the-

dark-web-2015-7/? r=US&IR=T#Xg01BPcbqoY4EWqA.97>. Accessed on: 27/2/2016

Borneo. (2015). Five individuals nabbed for terrorism activities. *The Borneo Post*. <http://www.theborneopost.com/2015/12/06/five-individuals-nabbed-for-terrorism-activities/#ixzz429HY8dlS>. Accessed on: 24/3/2016

Baron, B. F. (2004). Deterring donors: Anti-terrorist financing rules and American philanthropy. International Journal of Not-for-Profit Law. Vol. 6. No.2. Pp.1-32.

Barakat,I. (2014). IS: Islamic social media state of mind. *Alaraby*. <https://www.alaraby.co.uk/english/politics/2014/11/15/is-islamic-social-media-state-of-mind>. Accessed on: 12/3/2016.

BawaÉdy, ×. (2006). ÑrhaÉb al alaÑntarnt al khaÏar al qaÉdÊm. daÉr maÎyr. ÏabÑa al ÑËwlaÉ.

CBC News. (2015). ISIS has a magazine - what we can learn from Dabiq: Top Stories. *CBC News*. <http://www.cbc.ca/news/canada/hamilton/news/isis-has-a-magazine-what-we-can-learn-from-dabiq-top-stories-1.3336005>. Accessed on: 24/2/2016

Calmaur, K. (2016). Apple vs. the. FBI. *The Atlantic*. <http://www.theatlantic.com/national/archive/2016/02/apple-fbi-san-bernardino/463128>. Accessed on: 21/3/2016

Crethiplethi. (2014). ISIS's Propaganda Machine. *Crethiplethi*. < http://www.crethiplethi.com/isis-s-propaganda-machine/islamic-countries/syria-islamic-countries/2015/>. Accessed on: 14/3/2016

Conway, M. (2006). Terrorism and the Internet: new media—new threat?. *Parliamentary Affairs*. Vol. 59. No. 2. Pp. 283-298.

Drifter. (2004). Modern Hawala. *How to vanish*. <http://www.howtovanish.com/2009/09/modern-hawala>. Accessed on: 15/2/2016

Dearden. L. (2016). Isis supporters threaten UK with terror attacks in new propaganda video. *independent.* <http://www.independent.co.uk/news/uk/home-news/isis-supporters-threaten-london-with-terror-attacks-in-new-propaganda-video-a6969006.html>. Accessed on:4-6-2016

Dhanapal, S., Sabaruddin, J. S. (2015). Rule of law an initial analysis of security offences (Special Measures) Act (SOSMA) 2012. *IIUM Law Journal*. Vol.23. No. 1. Pp. 1-29

Eshpar, Y., Baram, G., Averbuch, A., Siboni, G., Cohen, D., Rotbart, A., Crosston. (2013). the Threat of Terrorist Organizations in Cyberspace. *Military and Strategic Affairs*. Vol. 5. No. 3, 2013, pp. 127-144

Edelman, J. (2014). How Social Media is Being Used for Terrorism. *Site pro news*. <http://www.sitepronews.com/2014/09/22/social-media-used-terrorism>. Accessed on: 12/2/2016.

Faith, D. C. (2011). The hawala system. *Global Security Studies*. Vol. 2. No. 1. Pp. 24-33

Fox News. (2014). Google Play store reportedly removes ISIS app. *Fox News*. <http://www.foxnews.com/tech/2014/06/19/google-play-store-removes-isis-app.html>. Accessed on: 23/2/2016.

Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium?. *Computers & Security*. Vol. 18. No. 1. Pp. 28-34

Goodman, S. E., Kirk, J. C., & Kirk, M. H. (2007). Cyberspace as a medium for terrorists. *Technological Forecasting and Social Change*. Vol. 74. No. 2. Pp. 193-210.

Gunaratnam, S. (2016). Court reminds Malaysians to desist IS during ex-govt servant's sentencing. *New straits.*<http://www.nst.com.my/news/2016/03/135132/court-reminds-malaysians-desist-during-ex-govt-servants-sentencing>. Accessed on: 4-3-2016

Greenberg, A. (2014). Hacher lexicon what is the dark web?. *Wired*. <http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web>. Accessed on: 12/3/2016

Hill, G. (2015). Cyber Caliphate Attacks Malaysia Airlines Website. *Security today*. <https://securitytoday.com/articles/2015/01/26/cyber-caliphate-attacks-malaysia-airlines-website.aspx?admgarea=ht.airport>. Accessed on: 27/2/2016

Hayward, J. (2015). Mystery Gunmen Attack ISIS Radio Station in Mosul. *breitbart.* <http://www.breitbart.com/national-security/2015/08/31/mystery-gunmen-attack-isis-radio-station-in-mosul/>. Accessed on: 19/3/2016

Harding, T. (2007). Terrorist use Google map to hit UK troops. *Telegraph*. <http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html>. Accessed on: 19/3/2016

Halkon, R. (2015). Paris attacks: ISIS terrorists may have used PlayStation 4s to plot atrocities. *Mirror.* <http://www.mirror.co.uk/news/world-news/paris-attacks-isis-terrorists-used-6836462>. Accessed on: 22/3/2016

Jost, P. M., & Sandhu, H. S. (2003). The hawala alternative remittance system and its role in money laundering. *Interpol. the Financial Crimes Enforcement Network in cooperation* with INTERPOL/FOPAC

Kennedy - Pipe, C., Clubb, G., & Mabon, S. (2015). Terrorism and political violence. *London*: Sage.

Lamothe, D. (2015). U.S. military social media accounts apparently hacked by Islamic State sympathizers. *Washington post.* <https://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers>. Accessed on: 28/2/2016

Leswing, K. (2016). Over half of Americans think Apple should unlock the San Bernardino shooter's iPhone. *Business Insider*. <http://www.businessinsider.my/over-half-of-americans-think-apple-should-unlock-san-bernardino-iphone-2016-2/#CPLIpf791Ex4w4id.99>. Accessed on: 19/3/2016

Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. *Center for Strategic & International Studies*. pp. 1-12

Minei, E., & Matusitz, J. (2012). Cyberspace as a new arena for terroristic propaganda: an updated examination. *Poiesis and Praxis*. Vol. 9. No.1. Pp.163-176.

QÉÍtaÉnyÊ, M., QÉÍtaÉnyÊ, M. (2014). Al qËwaÊ al khÉfyÊÉ lÊ daÉÑsh fÊy al'aÑlÉm al jadÊed. *jaÉmÊÑt al malÊk* sËÑwd.

Rouse, M. (2013). Definition of Bitcoin. *Tech target*. <http://whatis.techtarget.com/definition/Bitcoin>. Accessed on: 15/3/2016

SafÊr, ×. (2013). Al 'rhaÉb wa alÑËnf fÊy mËyzaÉn al sharÊÑh al 'slamÊyÉh wa al qaÉnwËn al ÑËwlaÉ. Dar al daËwha. qaÏar.

Sario, U, S. (2013). Lahad Datu: Eight charged in Tawau High Court over Sabah incursion. *The Star*. <http://www.thestar.com.my/news/nation/2013/03/21/lahad-datu-eight-charged-in-tawau-high-court-over-sabah-incursion-updated>. Accessed on: 24/3/2016

Siboni, G., Cohen, D., & Koren, T. (2015). The Islamic State's Strategy in Cyberspace. *Military and Strategic Affairs*. Vol. 7. No. 1, 2015, pp. 3-29

Shandra. (2012). History of cyber terrorism. *Blog*. <http://cyberterrorismlaw.blogspot.my/2012/03/history.html>. Accessed on: 18/3/2016

Simon, W. (2014). The operation of the security offences (special measure) acts 2014 and comparison with old internal security act 1948. herading a new democratic era or old win in a new bottle?. *International Journal of Technical Research and Applications*. www.ijtra.com Special Issue. e-ISSN: 2320-8163. Pp 78-83.

Trowbridge, A. (2014). "ISIS swiping hashtags as part of propaganda efforts". *Computer business review*. <http://www.cbsnews.com/news/isis-hijacks-unrelated-hashtags-in-attempt-to-spread-message>. Accessed on: 25/2/2016

Theohary, C. A. (2011). Terrorist use of the internet: Information operations in cyberspace. Washington. *DIANE Publishing*. March 8, 2011.

Veerasamy, N. (2009). Towards a Conceptual Framework for Cyber-terrorism. *4th International Conference on Information Warfare and Security*. Cape Town, South Africa. 26-27 March 2009. pp 10.

Weimann, G. (2004). www. terror. net: How modern terrorism uses the Internet. *United States Institute of Peace* . Vol. 31. No. 11. Pp. 1-11.

Weimann, G. (2014). New Terrorism and New Media. *Wilson Center Common Labs*.Vol. 2. Pp. 1-17.

WazaÉrt Al ’wqaÉf Al SwËrehÊ. (2014). Al ÑrhaÉb al ’alkÊtrËwny al thawËabit wa al motaghÊyraÉt. *baÑath baÉrtÊ*. < http://www.baathparty.sy/arabic/index.php?node=552&cat=1296&>. Accessed on: 3/1/2016

’aesar ÑaÏeÊh. (2014). Al Gra’m FÊe Úil Al MotÉgheÊrÉt Wa AlmotahawÊlÉt Al ÉqleÊmÉa Wa Al dwËÉleÊa,