Cyberterrorism’s Dilemma: Renewal of Conventional Terrorism

Nadiah Khaeriah Kadir
Magister Program, Faculty of Law, Universitas Hasanuddin, Indonesia

Abstract

Utilization of cyberspace is increasingly developing along with the advancement of information technology in the current era of globalization. borderless, low cost, fast access, encouraging terrorists to use cyberspace to facilitate their actions by combining direct attacks and through the internet network. The convergence of the physical and virtual world by these terrorists has resulted in the creation of new threats called cyberterrorism. This study aims to explain what cyberterrorism is, what they do, conventions that regulate cyberterrorism, and how to deal with cyberterrorism. This study used qualitative research methods with descriptive explanations sourced from journals, books, conventions, laws and regulations and other sources relating to cyberterrorism. The result of this study explained that cyberterrorism unlawful use of information, computer systems and networks to intimidate or coerce government, civilians for political or social purposes. Conventions governing cyberterrorism including United Nations Convention Against Transnational Organized Crimes, Budapest Conventions on Cybercrime.

Keywords: Conventional Terrorism, Cyberterrorism, Cyberspace, United Nations Conventions Against Transnational Organized Crimes.

RIKSAWAN INSTITUTE®

Introduction

The presence of communication technology provides convenience and benefits for humans as users to achieve effectiveness and efficiency in every activity, especially communication. Apart from benefits gained by advancing technology in using the internet, problems arise when the computer networks used by various parties are misused by certain parties for opposing interests, known as cybercrime (Maskun, 2013: 46).

One of cybercrime that’s very troubling and getting attention is cyberterrorism. The existence of cyberspace is easily accessible against radicalism by making cyberspace as a new tool and field for action. The use of cyberspace by radical organizations such as terrorists creates new threats to the international world.

Some terrorist groups' networks get benefits indirectly from the presence of internet-based technology that encompass many aspects, such as propaganda, recruitment and development networking. The internet not only makes it easier for terrorists to communicate, organize terrorist cells, share information, plan attacks and recruit others, but also being used as a tool to commit acts of terrorism (Gable, 2010).

Cyberterrorism was coined by cyberterrorists to characterize computer-based attacks against targets. Even though this attack happened in cyberspace, terrorists still use four ways of conventional terrorism. First, it is planned and not an action that arises from anger. Cyberterrorism attacks must be planned because they involve the development or acquisition of software to carry out attacks. Second, it is political and is designed to influence political structure. Cyber terrorists are hackers with political motivation, and their attacks have an impact on political structure. Third, the target is civilians and civil installations. cyber terrorists attacking civilian interests. Denning qualifies cyberterrorism as an attack that results in violence against people or property, or at least causes enough danger to cause fear (Prichard, 2004: 280)

There are several reasons why terrorists use cyberspace in their actions (Weimann, 2015: 313). Minimum resources required. Cyberterrorism is cheaper than conventional terrorism. All a terrorist needs is a personal computer and an online connection. Terrorists don't need to buy weapons and explosives. Instead, they can launch digital attacks through telephone lines, cable, or wireless connections. Minimum resources needed for such attacks (one person in front of a computer connected to the internet) help groups who have limited funds. Anonymity. Cyberterrorism is more anonymous than conventional terrorism. Most like internet users, terrorists use online nicknames or screen names or log on to websites as unknown guest users, which makes it more difficult for security agencies and police to track their true identities.

Methods

This study used qualitative research methods with descriptive explanations sourced from journals, books, conventions, laws and regulations and other sources relating to cyberterrorism. Secondary data collection techniques used as the foundation of this research are carried out by means of library study techniques, namely collecting legal material related to the source of literature relevant to the problem discussed by collecting, reading, and re-recording these legal materials which are then grouped systematically which related to the problem in writing this research.

Data analysis techniques performed by the authors in this study after the legal materials are collected and then analyzed using descriptive techniques by describing primary legal materials in the form of conventions, legislation and secondary legal materials in the form of research results, books, scientific journal texts , print and electronic mass media news and internet sites about cyberterrorism.

New Step on Conventional Terrorism

In the context of post 9/11, the threat of cyberterrorism was associated with Al-Qaeda and other terrorist organizations. Cyberterrorists are considered as individuals who understand computers that are looking for vulnerabilities and can be easily exploited (Cassim, 2012: 381). Al-Qaeda's use of the internet based on media such as television and magazines lately threaten the security of organizations and their members. Television has limited time to broadcast long and concise news as an application of their ideology. In fact, the media was unsafe by those who allow their message to be taken by interested parties and distort the facts that affect public opinion about their actions.

The internet then coined the term cyberterrorism where a group of terrorists used cyberspace (various internet applications) in carrying out their terrorist acts. The internet allows for rapid dissemination of information, little risk, low costs, from potential recruitment to prospective partners in terrorist organizations. Many of them use cyberspace, for example groups found by Abu Musab Al-Zarqawi from the Al-Qaeda faction in Saudi have almost never been in direct contact with the mass media, they focus their communication activities on cyberspace. This method prevents them from receiving widespread media attention. Paradoxically, the mass media themselves use the web to find traces and messages about the latest terrorism in cyberspace which will encourage the emergence of public opinion internationally.

For Al-Qaeda, the internet is not only a method for reaching safer and faster media, but is also a turning point for the rise of effective communication strategies compared to traditional media. For the first time cyberspace was able to enable direct communication between terrorists and their public. The Internet can fill the limitations of the mass media, and allow them to avoid a number of moral rules contained in the mass media that limit their actions (Sarinastiti, 2018: 42).

Cyberterrorism: Convergence of Terrorism and Cyberspace

As with defining terrorism, there is no universal definition of cyberterrorism. In concept, cyberterrorism isn't different from traditional terrorism, but has a cyber element. Some researchers argue that terrorism activities in cyberspace are considered cyberterrorism (Yunus, 2012: 149).

According to Denning (1999), definition of cyberterrorism 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 cyberterrorism, 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 cyberterrorism, depending on their impact".

The term of cyberterrorism was first coined by Barry Collin in the 1980s. Collin claims that the convergence of these two worlds, virtual and physical, makes cyberterrorism worth talking about. Cyberterrorism refers to two basic ideas, cyberspace and terrorism (Collin, 1997). Cyberspace is an abstract domain and describes the virtual world in which computers and networks operate. Cyberterrorism can be understood as the use of violence against information, computer systems, and networks that violate the law to intimidate or force governments, civilians, or segments, in the continuation of political or social objectives (Veerasamy, 2009).

Terrorism and the internet are interrelated in several ways. The internet has become a forum for individual terrorist and terrorist groups to spread their messages of hatred and violence and to communicate with one another and with their sympathizers. In addition, both individuals and groups can attempt to attack computer networks, for example to bring down planes, destroy infrastructure, destabilize the stock market, or uncover state secrets. First, the internet is a forum for terrorists to spread their message of hatred and violence, to communicate with each other and as a vehicle for coordinating psychological warfare against their enemies. Second, terrorists attack computer networks, including those on the Internet, in what became known as cyberterrorism or cyberwarfare. Nowadays, terrorists use and abuse the internet for their own benefit more than they attack (Weimann, 2006). This kind of convergence overcomes the existence of conventional terrorism and shifts to utilizing the internet or cyberspace as a new means and tools of terrorists.

Cyberspace as a Means and Tools by Terrorists

Cyberterrorism as one part of cybercrime divided into several forms, such as computers as targets, computers as accidental acts of a crime, and computers as a means of committing crimes. When a computer is the target of a crime, the criminal's purpose is to find information, cause damage to the computer. This crime makes the computer system a target to get information, to control the system without authorization, and involves hackers who perform fraud on the computer system to gain unauthorized access (illegal).

Next level, the computer was an accident for a crime. The computer is used as a store of information. Therefore, it can be said that in this second way, the computer contains evidence of violations of the law committed by hackers. With the discovery of data on a computer as evidence of a criminal act of terrorism that has been or is being planned, it is done by decrypting encrypted documents (files) on the perpetrators's computer.

The last is the computer as a means to commit crimes, which is used for crimes with an electronic system as a means to commit crimes. In general, this kind of crime is a conventional crime committed by computer. However, this mode has developed, where electronic crime has combined computers and the internet as a means to commit or facilitate conventional crimes. In case of cyberterrorism, computers as a means or tool by creating a homepage for propaganda, recruitment, collecting data / information from the private sector or confidential data and establishing relationships with other terrorist groups, and all activities using encrypted data (Astuti, 2015: 168).

Conventions governing Cyberterrorism

United Nations Conventions Against Transnational Organized Crime (UNCATOC)

Conceptually, transnational crime or transnational organized crime is a crime that crosses the country. This concept was first introduced internationally by the United Nations in the 1990s at a United Nations meeting which discussed matters relating to crime prevention. On November 15, 2000 at the 62nd plenary meeting in Palermo, Italy, United Nations ratified the convention against all forms of organized transnational crime or better known as the United Nations Convention Against Transnational Organized Crime (UNCATOC) (Airin, 2009: 19). In this Convention, the United Nations declared transnational crime as a large-scale and complex crime committed by groups of people, but loosely or tightly organized to enrich those who participated at the expense of society and its members.

In Article 3 of United Nations Convention relating to Transnational Crimes stipulates that organized transnational crime is:

1. crimes committed in more than one country;
2. performed in one country but preparation, planning, direction and supervision carried out in another country;
3. conducted in one country but involves criminal organizations / groups involved in crime in more than one country;
4. performed in one country but the effects / effects that are very substantial occur in other countries.

In 1995, the United Nations identified several types of transnational crime (Basaria Panjaitan, 2017: 6). there are money laundering, terrorism, theft of art and cultural objects, theft of intellectual property, illicit arms trafficking, aircraft hijacking, sea piracy insurance fraud, computer crime or cyber crime, environmental crime, trafficking in persons, trade in human body parts, illicit drug trafficking, fraudulent bankruptcy, infiltration of legal business, corruption, bribery of public or party officials.

Budapest Convention on Cybercrime

Because cyberterrorism is a crime committed in cyberspace, the convention on cybercrime is worth discussing. The convention on cybercrime is the Budapest Convention On Cybercrime. Budapest Convention On Cybercrime is an international convention created by the Council of Europe as a form of cooperation in dealing with cyber crime, which consists of 64 participating countries. This convention is also the first international agreement on crimes committed through the internet and other computer networks, specifically dealing with copyright infringement, computer-related fraud, child pornography, and network security violations. The main purpose of this Convention is to establish a joint policy in protecting the public against cyber crime, by adopting appropriate laws and encouraging international cooperation (Council Of Europe Portal, 2001).

Relating to cyberterrorism, cyberterrorists acts are criminalized by this Convention as part of achieving their goals. In article 2 on illegal access, cyber terrorists illegally access computer systems to obtain the information they need, for example their target attack profile. Furthermore, in Article 4 concerning data disruption, computer data is hacked by cyber terrorists to disrupt computer systems. And there are several articles regarding illegal tapping, system disruption, and misuse of equipment related to acts committed by terrorists.

United Nations Office on Drugs and Crime

Terrorists have knowledge of computers and use the internet regularly for various activities that support terrorism, such as propaganda, recruitment, communication, planning, etc. A recent report from the United Nations Office on Drugs and Crime (2013) that terrorists use the internet to: (1) Spreading propaganda related to instructions, explanations, justifications, or promotion of terrorist activities; (2) Incite violence; (3) Recruiting and radicalizing individuals; (4) Raise funds for assault through direct solicitation, e-commerce, exploitation of online payment instruments, and through charitable organizations; (5) Train followers about war tactics, using explosives and weapons; (6) Plan and coordinate attacks, often involving confidential communication between several parties.

Overcoming Cyberterrorism Actors

The fact that the internet and email are used as an ideal medium for communication of terrorists, raises the question of how intelligence agencies and law enforcement agencies of countries that seek to combat cyberterrorism can easily find and intercept such communications. There is a large amount of data and services available through the internet that can be used in investigations to counter terrorist using internet, as follows (UNODC, 2012: 61) :

Data collection. This phase involves collecting data through traditional investigative methods, such as information relating to the suspect, co-occupants, relevant colleagues or other colleagues and information collected through conventional monitoring activities of communication channels.

Research for additional information available through internet-based services. This phase involves requests to obtain information collected and stored in web-based e-commerce databases, communication services and networks, such as eBay, PayPal, Google and Facebook, as well as using specialized search engines such as www.123people. com. Data collected by this service through commonly used internet cookies also provide important information about many users from a single computer or mobile device.

The activities in phases 1 and 2 above provide information that can be combined to establish the profile of the individual or group that is being investigated and available for analysis during the next investigation phase. Request for a VoIP server. In this phase, law enforcement authorities request information from VoIP service providers relating to the person being investigated and affiliates or users of the same network device. Information collected in this phase can also be used as a smart filter for verifying the information obtained in the two previous phases. The working principle of VoIP is to convert analog sound obtained from speakers on a computer into digital data packages, then from a PC to be forwarded through a Hub / Router / ADSL Modem sent over the internet network and will be received by the destination through the same media. Or through a telephone medium forwarded to a phone adapter that is connected to the internet and can be received by the destination phone (Khilmy, 2013).

Analysis. Large volumes of data obtained from VoIP servers and various internet service providers analyzed to identify information for investigative purposes. This analysis can be facilitated by computer programs, which can filter information or provide graphical representations of digital data collected to highlight, inter alia, trends, chronology, the existence of organized groups or hierarchies, the geolocation of group members, or general factors among many users, such as a common source of financing.

Identification. After data is analyzed, it is necessary to identify subjects, for example on customer information linked to financial, VoIP, or email accounts.

Interception activities. Law enforcement authorities use interception tactics using digital communication channels. Interception activities can be carried out in connection with telecommunications services, such as fixed broadband, cellular broadband and wireless communications, as well as those relating to services provided by ISPs, such as email, chat and forum communication services.

Conclusion

Cyberterrorism is an act of terrorism by using the internet as a tool or media with a specific purpose. Cyberterrorism is categorized as a transnational crime because the crime is committed across national borders or it is said to be a transnational crime. To carry out the action, cyberterrorists use the internet to hack into the target computer system of attacks, damage infrastructure, for propaganda and certain purposes. There are several conventions that govern cyber terrorism such as United Nations Convention Against Transnational Organized Crimes which explain the types of organized crime, Budapest Conventions on Cybercrime, and United Nations Convention on Drugs and Crimes.***

References

Airin, Dyah Ridhul. 2009. Kejahatan Lintas Negara Terorganisir Di Bidang Perikanan Oleh Nelayan Asing Dan Penegakan Hukumnya. Thesis of Graduate School Hasanuddin University. p. 19.

Astuti, Sri Ayu. 2015. Law Enforcement of Cyber Terrorism in Indonesia. Jurnal Rechtsidee Vol 2 No. 2 p.168.

Cassim, F. 2012. Addressing the Spectre Of Cyber Terrorism: A Comparative Perspective. Journal of PER Vol. 15 No. 2. P.381.

Collin, B. 1997. The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. 11TH Annual International Symposium on Criminal Justice Issues. http://www.crimeresearch.org/library/ cyberter.htm. Accessed on 9 July 2020.

Council Of Europe Portal. 2001. Convention On Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/ treaty/185. Accessed on 6 July 2020.

Denning, D. 1999. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. https://www.rand.org/ content/dam/rand/pubs/monograph_reports/MR1382/MR1382.c h8.pdf. Accessed on 9 July 2020.

Gable, Kelly A. 2010. Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. Vanderbilt Journal of Transnational Law. https://www.vanderbilt.

edu/wp-content/uploads/sites/78/Gable_camera_ready_final.pdf Accessed on 8 July 2020.

Khilmy, Zulfa. 2013. Voice Over Internet Protocol. https://www.kompasiana.com/zulfakhilmy/552987be6ea834c56c552cfa/ voice-over-internet-protocol. Accessed on 11 July 2020.

Maskun. 2013. Kejahatan Siber (Cyber Crime) Suatu Pengantar. Jakarta : Prenada Media Group. p. 46.

Office on Drugs and Crime. 2013. The Use of the Internet for Terrorist Purposes. New York: United Nations. www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf. Accessed on 10 July 2020.

Panjaitan, Basaria. 2017. Mengungkap Jaringan Kejahatan Transnasional. Bandung : PT Refika Aditama.

Prichard, Janet J. 2004. Cyber Terrorism : A Study of The Extent of Coverage in Computer Security Textbooks. Journal of Information Technology Education. Vol 3 p. 280.

Sarinastiti, Eska Nia. 2018. Internet dan Terorisme : Menguatnya Aksi Global Cyber Terrorism Melalui New Media. Jurnal Gama Societa. Vol. 1 No. 1.

UNODC. 2012. The Use Of The Internet For Terrorist Purposes. New York : United Nations.

Veerasamy, N. 2009. Towards a Conceptual Framework for Cyberterrorism. Council for Scientific and Industrial Research. http://researchspace.csir.co.za/dspace/bitstream/handle/10204/3335/Veerasamy_2009.pdf?sequence=1&isAllowed=y. Diakses pada 10 July 2020.

Weimann, Gabriel. 2006. Terror in Cyberspace. www.docit.tips_terror-in-cyberspace-pdf-download-available-.pdf. Accessed on 7 July 2020.

Weimann, Gabriel. 2015. Terrorism in Cyberspace : The Next Generation. New York : Columbia University Press.

Yunus, Zahri. 2012. A Dynamic Cyber-terrorism Framework. International Journal of Computer Science and Information Security. Vol. 10. No. 2. Hlm. 149.