Cyber terrorism handling in Indonesia

Muhammad Nadjib
Hafied Cangara
Department of Communication, Hasanuddin University, Indonesia

Keywords
Indonesia, cyber media, terrorism, radicalism, youth.

Abstract

Terrorism has existed since the 18th century before the outbreak of the French Revolution, but the issue of terrorism became more alarming since the bombing of the World Trade Center in September 11, 2001. Since then US President Bush had declared war against terrorists around the world. As a response to this declaration, the terrorists led by the Al-Qaeda, made a challenge not only to Western countries considered enemies but also to some Islamic countries they considered deviate from pure ideology of Islam such as Indonesia, Pakistan, Libya, Yemen, and other Islamic countries.

Indonesia became the world's fourth largest target of bombings after the United States, Nigeria and Iraq. From 1981- 2016, 336 people killed in terrorist attacks in Indonesia. Bali bombing in October 12, 2002 killed 202 people, and recent bombing in the commercial center Sarinah Jakarta killed seven people, still many others were wounded. Based on the notes of Indonesian National Agency for Terrorism Handling, up to 2014 there were 9.800 radical sites and 46.000 twitter accounts in the internet. The Indonesian national police agents had responded to the anarchists by chasing the terrorists and killed 112 terrorists who were directly involved in the anarchy. Subjects of terrors in Indonesia were not strangers, but Indonesian citizens coming from young family with marginal social background, who received financial support from international terrorist networks via the Internet.

The use of internet by terrorists had rebirth a concept of cyber terrorism, which is a convergence between internet and terrorism. Cyber terrorism was used by terrorists as global communication media for propaganda, fundraising, communication, information gathering, spreading violence issues and psychological warfare. Because cyber terrorism is multi-dimensional, therefore the government of Indonesia also handled the issue with a multi-dimensional approach, starting from the formation of elite military detachment (Densus) 88 for anti-terrorists by the National Agency for Terrorism Handling, established anti-terrorist constitution, international cooperation on anti-terrorist handling, closing of sites and radical twit accounts, actively carrying out social campaigns targeting young Indonesian teenagers from which 98% were active internet users sensitive to radical standpoint influences.

Introduction

Terrorism has existed since the 18th century before the outbreak of the French Revolution, but the issue of terrorism became more alarming since the bombing of the World Trade Center in September 11, 2001. Since then US President Bush had declared war against terrorists around the world. As a response to this declaration, the terrorists led by the Al-Qaeda, made a challenge not only to Western countries considered enemies but also to some Islamic countries they considered deviate from pure ideology of Islam such as Indonesia, Pakistan, Libya, Yemen, and other Islamic countries.

Terrorism currently occurs as a global phenomenon threatening countries all over the world, covering economic, social, and government realms. Though it is purely as a security term that is most visible to the public, countries that do not deal with the problem of terrorism effectively will be trapped as 'weak states' as they cannot protect their peoples and achieve international standards to secure their regional environment for a peaceful world.

In many countries, terrorism is not a new trend and has existed as consequence of contradiction and injustice existing in the world. Terrorism may be the continuation of a long historical violence arose in domestic realm, and find a momentum to emerge along with global change. The attack on World Trade Centre in New York City (2011) is regarded a starting point for a new war on terrorism. Since then, terrorism has spread all over the world with different characteristics; it is predominantly based on ideological or religious motives. In this regard, the Islamic factor plays an important part. In many attacks, terrorist hide behind Islam emblems, attract members with the reasons of securing Islam from being humiliated or marginalized.

Indonesia as the most populous Muslim country in the world is not free from the danger of terrorism. Foreign observers mentioned Indonesia as a safe haven for terrorist groups, due to her domestic vulnerabilities. The situation became worse when Indonesia entered the transition to democracy following former president Soeharto's resignation in 1998.

Terrorism indeed is a major challenge to all post-Soeharto governments, from President B.J. Habibie, to Abdurrahman Wahid, to Megawati Soekarnoputeri and to Susilo Bambang Yudhoyono. Subsequently, they applied policies to cope with terrorism during their administration. A comprehensive assessment is needed on Indonesia's counterterrorism policy, which is currently being implemented, to ensure Indonesia's transition to democracy will be stable and not snared as a failed state. Such counterterrorism policy, to be applied properly, will free Indonesia from the trap of violence that has compromised its security. The worst scenario envisaged is a possible disintegration as a result of never-ending spiral of conflict. (Cite ???)

In Jokowi era, counter terrorism policy combine two contrast strategies, one approach was shutting off hundreds of websites suspected in aligned with terrorist movement, close down an organization which is suspected a hard liner diffusing information supporting terrors ideology and criticizing the national ideology of Pancasila. Second approach is rather persuasive approach to community leaders, party leaders, and religious leaders and reinforces the values of "Pancasila" as the basic principle of Indonesia, as glue to all parties and all Tribes, religions, Race and Customs (community group) called SARA. This approach is conducted through seminars information disseminations through all government, public and private TV media and online social media. In most presidential speech "pancasila" issue is always mentioned as a single and the only ideology which is able to unite various tribes, race, language, community, and religious group, living in scattered islands, in order to stimulate motivation and commitment to live in harmony in Indonesia, even if the result of the approach is still questionable. Private and national media captured this specific part of president's speech and rebroadcast them repeatedly like a state advertisement.

Many countries in the world such as the United States, Britain, and other European countries under the Umbrella of NATO, Some Asian countries like Malaysia, Japan, and South Korea are very concerned with cyber terrorism intrusion to their citizens and to their countries that is why they have clear and strong policy and constitution against terrorist activities. NATO for example had conducted various conferences, seminars and workshops on prevention from cyber terrorism. Participating countries contribute to the seminars by introducing their own policy of combating cyber terrorism. Most of them work fine, but for a long time, Indonesia's' system is considered weak, for its insufficient constitution and regulation to combat and eradicate terrorism which makes Indonesia fertile land to disseminate terrorist propaganda, to obtain financial support for terrorist purposes, and to conduct terrors on individuals or on state personnel regarded unfriendly towards terrorist ideology, such as police men, and legal persecutor, and public in general.

Cyber terrorism is defined

In assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats from Center for Strategic and International Studies released in December 2002: Lewis defined cyber terrorism as is a prohibited assaults and hazards against computer systems, computer networks, and the Internet. Another definition was given by Ct. Andieny (1) Cyber terrorism is the usage of any information technology by terrorists. The objective of cyber terror as reported in Andieny is the use of cyber space to initiate terror by threatening or forcing a government or its citizens in continuance of objectives.

George Jarvis, in an academician perspective, restated a more comprehensive definition of cyber terrorism, one of the most popular and the most widely cited definition in cyber terrorism context that represents an academic's points of view. As a Naval Post Graduate School, Professor Dorothy Denning defined cyber terrorism as: "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."
With Dennings' definition, cyber terrorism requires the following elements.

1. Participants are non-state actors
2. Attacks are computer-based with a big payload (highly damaging) on IT-based infrastructures
3. Victims are either governments or societies
4. Attackers' goals are either political or social
5. Destruction/disruption is done against digital property rather than persons or physical property
6. Cyber-terrorism is terrorism but limited within the scope of cyberspace.

A critique on the first element of non-state actor or participant was stated by (Conway 11); Professor Denning made it clear that non-state actors of that state-sponsored terrorist organization do not fit this definition. For Conway Cyber terror is not particularly addressed to individual only but some other terrors are coordinated by states. Conway, an international security lecturer describes cyber-terrorism as the union of two fears: Fear of technology, and Fear of terrorism.

In A NATO conference conducted in Ankara Turkey from 5-9 May 2014, (2), Director Robert Mueller, in a Report of terrorist Use of Cyberspace, detailed the nature of cyber terrorism in its relation to cyber terrorist as follows:

- In 10 years' time al Qaeda's online presence is equivalent to their physical presence
- Extremists use cyberspace for more than recruitment or radicalization
- Cyberspace is being used to incite terrorism/terrorist acts
- Thousands of extremist websites target an undisclosed number of captive audience members in promoting violence.
- Viewers to these extremist websites can learn to build backpack bombs and bio-weapons through posted videos.
- Social networking has been useful in linking terrorist plotters and plans.

With this detail and these characteristics in mind, cyber terrorism is not simply defined as an attack intended to damage computer data, cyber space, and internet facilities, but also an act of using computer, cyber space, and internet by terrorists to promote violence, recruit terrorist members, spread terrors, link terrorist plotters and plans, using videos posted through internet to build back pack bombs.

The association of Internet provider in Indonesia described cyber terrorism as a threat that is aimed at disturbing the general community. Spamming and Abusing were included in this description. Spamming is an electronic letter in advertorial form sent to an electronic mail owner without the consent of the owner. Besides that, spamming also addressed ones' server owner to attack a target server. While abusing is an act of a unlawful use of internet such as distributed denial on service, hacking, humiliating, distributing issues on discrimination of race, religion, and ethnics, and pornography.

In Indonesian Language"*Terorisme Mayantara*", equivalent to (Cyber terrorism in English) is a form of planned activity politically motivated to attack information, computer system, computer program and data which causes a great loss and victims of innocent people committed by a group or a person. The role of new media in this argument of the association is considered a shift from traditional to modern terrorism resulting a number of new paradigms in Indonesian terrorism movement, such as the birth of Phantom Cell Network, Leaderless Resistance, and Lone wolves terrorist categories with their own way of committing terrorism and cyber terrorism.

Cyber terrorism in Indonesia

In Indonesian terrorism case, a cyber terrorism related to the above definition was recognized between the first and the second Bali Bombing, when Abdul Aziz or most widely known as Imam Samudra planned the second Bali Bombing from a prison using a lap top to communicate and coordinate his cadres who were still free out of prison. The laptop was smuggled by Agung Prabowo and Agung Setiyadi two friends of Imam Samudra with the help of a prison warden, in a visit to prison. Imam samudra used the laptop access the Internet for communicating and coordinating his friends to plan the second attack later known as the second Bali Bombing.

Sulastri Osman and Navhat Nuraniyah in their report: (3) revealed a final message of Imam Samudra, the actor of the first Bali bombing. The message was we should be "hackers, bombers and fighters". With this statement, it is clear, that the future plan of terrorist is shifting from traditional to virtual, involving cyber attack and hacking to facilitate their strategy of conducting real fighting and bombing. In 2014, more than five years after Samudra was executed for his role in the 2002 terrorist attacks in Bali, a new generation of like-minded extremists have realized his last will as they acquire the technological skills necessary to exploit online tools to facilitate their offline terrorist operations.(3)

The developments of Internet penetration paralleled with the mushrooming of smart phones have contributed to the rise of terrorism-related activities online. Sulastri (3) After the Jakarta Hotel bombing in 2009, Indonesia police had exercised a heavy suppression on Indonesian terrorists and their organization, but new generation of tech-savvy terrorist at the same time had also rebirth. The rebirth of this new terrorist generation is not simply a shift into a cyber realm following the tough police measures, but also influenced by the way the new actors of a technologically savvy generation comfortable with their high-tech devices which are mobile and constantly connected.

Cyber terrorism in Indonesia is recognized as "terrorismemayantara". *Mayantara*is an Indonesian word for Cyber. Therefore *terrorismemayantara* is cyber terrorism in English. This new terrorism is different from traditional terrorism movement. Bali Bombing one for example was a traditional terrorism indicated by the presence of personnel and a clear command. Agus(4)

New terrorism rose and developed as a result of Internet technology in which they use to perform their terror. Example of the new terrorism was Bali Bombing II, planned, coordinated by Abdul Azisor Imam Samudra through internet media. The second Bali Bombing broke when Imam Samudra was in prison. He planned, controlled, coordinated and monitored the second Bali bombing attack by communicating and coordinating his terrorist fellows outside of the prison via Internet with a laptop smuggled by a friend into prison without the consent of the guard.

Robert Raffaele reported on an open block of news paper article of US Fed News Service, including US State News on 23 August 2006(5) that: Agung Prabowo and Agung Setyadi were arrested in separate raids in Java province. Indonesian authorities say Setyadi and a prison warden smuggled a laptop computer into the death row cell of Imam Samudra in July of 2005. Samudrawas the mastermind of the October 2002 nightclub bombings in Bali. 202 people were killed in those attacks, most of them foreign tourists. Investigators say Samudra used the laptop to chat from his cell with Setyadi and other Islamic extremists for months. Police say the men's online conversations included how to fraudulently use credit cards online to transfer money for terror attacks.

VOA NEWS: Indonesian police charge two suspects with cyber-terrorism (6) reported three more bombs exploded in Bali nightspots last October, after the discussion took place. And that was the beginning of the new terrorist attack in Indonesia stipulated by the introduction of the new technology. Samudra and two other men were sentenced to death for the 2002 attacks, meanwhile Agung Prabowo who was accused of helping create a web site that outlined the best way to assassinate foreigners in Bali, including shooting people "several times" in the heart and head.

Cyber terrorism in Indonesia was not simply a shift from traditional to modern terrorism, but it is a reflection of the new technologically literate generation adopting the new high-tech devices with all its characteristics: such as fast, accurate, mobile and connected. All of these characteristics certainly have facilitated terrorists to reach out to and recruit new followers online. According to 2013 survey, Indonesia in 2006 had already had 75 million Internet users, an increase of 22% from proceeding year. (6)
Sigit Indrajit, Seva Rianohad a contact with others through their posting on Rohingya situation, communicating their needs to revenge Rohingya. With the aid of internet, they even planned to attack the embassy over face book. In the same report, police confirmed that the amateur cell learned to make pipe bombs, intended for attacks, from explosive manual they learned from online source. Another example was Pepi Fernando, the mastermind of 2011 book bombs learned to put together explosives from the Internet. (6)

Riski Gunawan, a known militant linked to the cell, and Mawan Kurniawan, an IT specialist and supporter of imprisoned extremist figures, had made away with over US$625.000 through credit card fraud and hacking activities to fund ongoing terrorists activities in Poso, Central Sulawesi. More cases of

attacks on government websites were the hacking of the police website in 2011, the state military website in late 2012 and early 2013 by Poso terrorist to send a threat to counter terrorism authorities. (6)

All of those above examples showed how the Internet facilitate the activities of terrorist such as recruitment of new members online, plan to attack the embassy, learn to make pipe bombs, learn to put together explosives from internet, break into a personal or institutional bank account to withdraw money for terror purposes, hacking the police website in 2011 and the military website 2012, and send a threat to counter terrorism authorities in 2013. (7)

Condition facilitating cyber threat in Indonesia

Indonesia became the world's fourth largest target of bombings after the United States, Nigeria and Iraq. From 1981- 2016, 336 people killed in terrorist attacks in Indonesia. Bali bombing in October 12, 2002 killed 202 people, and recent bombing in the commercial center *Sarinah* Jakarta killed seven people, still many others were wounded. Based on the notes of Indonesian National Agency for Terrorism Handling, up to 2014 there were 9.800 radical sites and 46.000 twitter accounts in the Internet.

The World Summit Information Society (WSIS) in 2003 had declared that at least half of the world's population has Internet access in 2015. Since the Telecommunications Act was adopted in 1999, telecommunications sector in Indonesia entered a new phase. The telecommunications industry is growing rapidly. Currently there are ten telecommunications operator with 180 mobile phone users. High number of mobile phone subscribers also following by internet. The growth of Internet penetration in Indonesia is 12.5% or by 30 million users in 2010 [3].

This growth rate was lower among other Asian countries, but in terms of number, that number ranked the top in Southeast Asia Region, or the highest ranked five in Asia Region, and therefore it is also vulnerable to cyber attacks. Indonesia's population is estimated approximately 255 million in 2015. In 2011 Internet users in Indonesian had reached 55 millions. It means government should be able to provide Internet access to 70 million people. In the meantime Indonesian government should be more aware, because the high number of internet users and internet utilization for life will increase the frequency of the inappropriate usage of internet for terrorist purposes.

In a study conducted by Jennifer Yang Hui (8), a Saudi researcher Khaled al-Faram estimated that there are currently 5,600 websites that disseminate AlQaeda influenced ideology around the world, and that the number is increasing by 900 every year. Noordin M Top, a Jemaah Islamiyyah (JI) leader who orchestrated several major bombings in Indonesia, was believed to have ordered the creation of a website with content on the best ways to attack foreigners in addition to the favored places to attack foreigners in Jakarta.

The arrest of Abdul Basheer s/o Abdul Kader in Singapore is also a good example. Abdul Basheer was a former law lecturer who aspired to join mujahidin fighters in Afghanistan after being influenced by extremist ideas from the Internet, thus demonstrating the potential of the Internet as a tool for propaganda and recruitment. These examples are all instances of the phenomenon of cyber terrorism.

Special cases and handling of cyber terrorism in Indonesia

Because cyber terrorism is multi-dimensional, therefore the government of Indonesia also handled the issue with a multi-dimensional approach, starting from the formation of elite military detachment *(Densus)* 88 for anti-terrorists by the National Agency for Terrorism Handling, established anti-terrorist constitution, international cooperation on anti-terrorist handling, closing of sites and radical twit accounts, actively carrying out social campaigns targeting young Indonesian teenagers from which 98% were active internet users sensitive to radical standpoint influences.

Formation of Elite Military Detachment

Special Detachment 88 (***Detasemen Khusus 88***), **Delta 88**, or **Densus 88**, is an Indonesian Special Forces counter-terrorism squad, and part of the Indonesian Police Force. Formed on 30 June 2003, after the 2002 Bali bombings, it is funded, equipped, and trained by the United States[3] and Australia.[4]The unit has worked with considerable success against the jihadi terrorist cells linked to Central Java–based Islamist movement Jemaah Islamiyah.[5]

Detachment 88 has disrupted the activities of Central Java–based Islamist movement Jemaah Islamiyah (JI) and many of its top operatives have been arrested or killed.[5] Abu Dujana, suspected leader

of JI's military wing and its possible emir, was apprehended on June 9, 2007.[10]Azahari Husin was shot and killed in 2005. The Indonesian terrorist organization suffered a further blow when arguably its last surviving and at-large prominent figure, Noordin Mohammad Top was killed in a shootout with Detachment 88 on September 17, 2009 at Solo, Central Java.

Detachment 88 is assisted by foreign agencies, including the Australian Federal Police, in forensic sciences including DNA analysis, and communications monitoring. In pre-emptive strikes in Java, the unit thwarted attack plans to material assembly.[5]Detachment 88 operators were involved in an operation in Poso, where 10 people, including a policeman, were killed in a gunfight during a high-risk arrest operation on January 22, 2007.[11]

In 2007, Detachment 88 arrested and interrogated West Papuan human rights lawyer, Iwangin SabarOlif, and charged him with incitement and insulting the head of state, because he sent an SMS text message critical of the Indonesian military and president.[3]Six members of a little-known terror cell called Katibah GR, or Cell GR, were arrested by counter- terrorism unit Densus 88 after carrying out a raid in Batam in August 2016. Police said their leader had been planning a rocket attack on Marina Bay, Singapore together with a Syrian-based Indonesian ISIS militant.[12]

Detachment 88 however deals with the terrorist and tried to stop their activities by identifying the persons regarded as terrorists, finding its network and arrest those who have been identified as members of individual terrorist or terrorist organization. Detachment does not really deal with cyber terrors, in terms of a threat on internet, social media or cyber media, but they still need cyber technology in the process of identifying the suspects, searching their networks, determining their presence and planning the arrest and or the execution. If the radical websites and twitter accounts of all terrorist and their network were eventually closed down, then the search of their network, and their activities and their plan will be difficult to trace. (The hydra effect of closing down the terrorist websites).

Establish Antiterrorist Constitution

Indonesian government had established a Constitution number 36, year 1999, about telecommunication, one of which can be used to organize appropriate and protect from illegal use of Internet technology. Chapter 21 of this constitution covered a regulation that forbid to conduct telecommunication activities contradictory to the public interest, morality, peace, and public orderliness.

Although this constitution is considered too general, for the time being, it is considered quite effective in handling violation in telecommunication use in order to regulate negative contents especially containing terrorist propaganda, provocation, agitation, and threat to individual or community in general. One of the provocative issue was handled with this constitution was a controversial film made by a Dutch politician Geert Wilders which was considered containing provocative content related to SARA (Suku, agama, ras, danadat) (Tribe, religion, race, and custom), which is a very sensitive issue in a multi varied population of Indonesia. This film offended the tranquility of Islam religion followers, the majority religion followers in Indonesia.

Because this constitution was too general and was applicable for limited cases, meanwhile the use of internet is rapidly proliferating, therefore this constitution is considered insufficient to cover most types of violations on the use of internet and related technology. Responding to the ever increasing cases of internet crimes and violations, the government of Indonesia strengthens the internet content regulation with the establishment of Constitution Number 11, year 2008 containing information and electronic transaction. With this constitution, it is made clear in chapter 27 article 4 "that everyone who deliberately and without a right to distribute and/or transmit and or make possible an electronic information with exploitation and threat be accessed; and in chapter 28 article 2 which stated "every one who deliberately and without a right to distribute and/or transmit information which causes hatred or adversary to individual or group of people because of tribe, religion, race, and inter group community… is regulated under this constitution.

Nevertheless, despite the challenges facing counterterrorism policing, there are equally opportunities forcounterterrorism innovation on online and social media platforms. Among other things, law enforcement agencies could leverage such platforms to gather intelligence. Advanced analytics tools such as sentiment analysis and implicit profiling can help trawl through vast amounts of data online. Much like in the real world, good intelligence lies at the crux of effective counterterrorism policing online.

However, in using such tools, restraint and accountability need to be prioritized to avoid the moral hazards of over-surveillance. Also, trained human analysts need to be present to help interpret the data collected and distil meaningful intelligence. Ultimately, what is needed is a repertoire of responses to the key concern of extremist content in cyberspace, especially the incitement to violence. While a special law to punish individuals who incite violence online can certainly benefit law enforcement, online communities can also be encouraged to conduct self-policing. Particularly if the Internet is to remain open, there is no need for strict laws to govern every concern since not every dubious activity online translates into a security threat. Self-policing also means that wider education regarding the dangers of extremist content and extremist individuals has to take place alongside the development of norms online.

A way forward is for counterterrorism agencies to not merely see the risks and dangers associated with online and social media but also the opportunities that the same tools can lend them. That said, Samudra's call for his supporters to be hackers, bombers and fighters should act as a reminder that terrorist operations straddle the online and offline worlds simultaneously. Accordingly, any counterterrorism policing efforts online have to account for offline dynamics as well. Sulastri Osman is Research Fellow and Navhat Nuraniyah is Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies(RSIS), Nanyang Technological University.

International Cooperation on Anti terror handling.

Politically, Indonesia has free and active principle; it is stated in the preamble of the constitution. Indonesia has collaborated with international parties on the issue of cyber security. For cyber security international cooperation, Indonesia has become a Full Member of the Asia Pacific and APCERT FIRST (Forum for Incident Response and Security Team) of the world. Indonesia also has become a Full Member and founder of the OIC-CERT (Organization of the Islamic Conference-CERT).International cooperation can also be interpreted in an effort to participate or agreed to an international agreement. Indonesia was also involved in the ratification of European Union of Convention of Cybercrime. The convention held on 23 November 2001 in Budapest, intended to discuss thoroughly the threats facing the international world of cyberspace-related crimes. This convention has been agreed that the Convention on Cybercrime included in the European Treaty Series No. 185.

Indonesian people with majority of Moslem population carefully observe the development of terrorism issue in Muslim world not only from the occurring conflicts, but also the democratic dynamics occurring in Turkey, Egypt, or Palestine. In those three countries, and also in other several countries in the Middle East, political Islam achieves significant support, and, in fact, the Islamist wins the current general election in Turkey and Palestine. The Islamic group views that the Western countries apply double standards when witnessing the success of Islamic parties in the democratic life when most of the Western countries refuse to acknowledge as is occurring in Egypt.

The contradiction could be seen also in the Algerian tragedy which happened due to riots after the success of Front Islamique du Salvation (FIS). Turkey is one model that should be taken into consideration, which shows that the victory of the Islamic-rooted Justice and Development Party (AKP) could bring stability and improve the welfare of the population. In Palestine, Hamas is presented with the difficult task of establishing national integration along with Fatah and other PLO factions. The new political changes in Palestine bring significant inspiration since a group which has been branded as terrorist has now become the authoritative government, when Hamas changed its strategy, i.e. "from bullet to ballot".

Following the long history of Israel's oppression, Hamas concludes that the legitimacy obtained from the ballots is more effective than bullets they fired. Their aim, of course, is to achieve an independent and sovereign Palestinian state. If the democracy practiced by Hamas is being ignored and the Palestine democratization process is denied, new forms of terrorism will emerge, and the repercussion will have impact on Indonesia as well. The radical Islamic groups will obtain more proof that the secular principles of Western countries do not provide peaceful solutions to settle their problems completely and genuinely.

Closing of sites and radical twit accounts,

During the election of the Governor of Jakarta, the political tension was intensified. A competition between parties, tribe, religion, race, and community groups were escalating because the candidate competing for the position came from different ethnic, race, religion. During the campaign, although it was stated in the rules of the campaign that issues of SARA which stands for Tribe, Religion, Race, and Ethnicity, should not be used for campaign material as they were very sensitive issue and could easily provoke conflict, these issues were unavoidable. In mainstream media which are directly relayed on TV, candidates could refrain themselves from attacking other candidate with SARA issues. But in social media, in websites in Internet disputes of race, religions, those media are available for free for everyone, and allowed open interaction and communication among members of the society regardless of their background.

To some extent this demonstration were considered a threat to the integrity of the nation, and to democracy, but for majority of Muslim population this was a very peaceful demonstration, and peaceful approach requesting the government to protect the religious rights of Muslim population from being insulted by other religious holder. The government was put in cross road between listening to the voice of majority and protecting the minority who have the same rights to live in peace in Indonesia.

The tension of political climate was very high and the social media was full of insults, hatred, defamation, offences and breaches of regulation. Many websites were created by either individual or group of people, to attack individual or organization. Those websites carried messages full of insult addressed to their religion, race, and ethnicity rivals. These discourses were very sensitive and easily stimulate conflict among the members of different race, religion and ethnicity. The government, in response to the situation, through the ministry of Communication and Information decided to control the conflict escalation stimulated over the Internet and shut down hundreds of twit accounts, websites or blogs potentially triggering conflicts and disintegrate the nation.

The Social unrest triggered by media and social media continued on to a street demonstration involving millions of Muslims from various organization and parties. It was considered a warning to rival or opposition candidate to reconsider his candidacy to the governor of Jakarta. The Internet and the social media again becomes an object of intensive inspection, from which many discourses were indicated sensitive to create conflict, and of which were also addressed to the government and even to the basic principles of our nation Pancasila. This is the reason an Islam organization "Hizbuttahrir" was closed down by the government for being measured a radical organization.

To some extent, the act of closing down websites, twit accounts, and an organization could be an instant panacea for creating peace on surface, but in the long run this treatment would create a prolong unrest challenge in society for the following reasons, called the Hydra Effect:

The Hydra Effect: What aims to block malignant content may create a more dangerous beast.
Content may just be re-hosted outside of the countries' jurisdiction.
Content creator, server hosting and domain registration may be in three separate locations.
Forces countries to utilize diplomatic channels.
Freedom of speech: Some content may be unappealing, but is not necessarily illegal.
Blocking content may tie up the intelligence community and law enforcement agencies
An impossible pursuit?
Chance of missing real and imminent threats?
Focus on one brand, leaving others free from detection and investigation?

Rather than staying in uncertain dilemma, the government had to respond immediately, with some alternative responses. One response by reducing the escalating disputes on the cyber media, others were chasing figures potential to provoke public for further demonstration, and still other approach were through persuasive method to young people and to all government and private institutions by reinforcement of the basic values of Pancasila, and international cooperation.

Actively Carrying Out Social Campaigns Targeting Young Indonesian Teenagers.

Through BNPT (National Board of Terrorism Handling) proposed a program called "Peace program in Cyber world". This program is conducted in various provinces in Indonesia. The objective of

the program was to introduce a perspective of terrorism handling in cyberspace, and establishing a networked cooperation among the young lovers of cyber-world. With cooperation (see Agus 170).

BNPT in cooperation with the Department of Communication and Information had conducted a program to go around the provinces and Regencies in Indonesia and established a "peaceful communication network" in a website portal www.damai.id. Through this website this cooperation had established "peaceful community network" with thousands members. They commit to create contents of peace and love NKRI (Indonesian Republic Union State), and tried to combat terrorist provocation in Internet. This organization also organized contra narration of provocative messages or issues on mass media, and publicized printed and audiovisual messages to support their mission of peaceful cyber world.

Federal Government Efforts to Address Cyber terrorism (Congressional Research service). It should be noted that the actions associated with the organizations listed below could be conducted by employees of the federal government or by civilian contract personnel.

- Central Intelligence Agency (CIA): development, surveillance, and analysis of websites, commonly referred to as honey pots, for purposes of attracting existing and potential jihadists searching for forums to discuss terrorism-related activities.23
- National Security Agency (NSA): surveillance of websites and rendering them inaccessible.24
- Department of Defense (DOD): surveillance of websites focused on discussions of perceived vulnerabilities of overseas U.S. military facilities or operational capabilities and disabling those that present a threat to operations.25
- Department of Justice (DOJ): development of polices and guidelines for creating, interacting within, surveilling, and rendering inaccessible websites created by individuals wishing to use the Internet as a forum for inciting or planning terrorism-related activities.
- Federal Bureau of Investigation (FBI): monitoring of websites and analysis of information for purposes of determining possible terrorist plans and threats to U.S. security interests.26
- Department of Homeland Security (DHS): monitoring of websites and analysis of information for purposes of determining possible threats to the homeland.27

Conclusion

Indonesia as a multi ethnic, multi religion, multi race, and multi ethnic population had always been sensitive from influence of change of policy, including the change of policy in cyber terrorism issues. Although Indonesia has become a Full Member of the Asia Pacific and APCERT FIRST (Forum for Incident Response and Security Team) of the world, Indonesia also became a Full Member and founder of the OIC-CERT (Organization of the Islamic Conference-CERT). These two organization do not always have exactly the same vision on cyber terrorism handling, because they have different background and different ideology when discussing about terrorist and Islam, for Indonesia, this issue is a very sensitive national issue and people and religious issue which has no instant solution.

Besides its international cooperation, Indonesia has specific programs for combating cyber terrorism, such as legal and constitutional approach, closing websites and radical organization and actively carrying social campaign targeting Indonesia teenagers. Closing websites and organization, and legal and constitutional approach have not been proved effective. A number of problems, such as insufficient constitution and regulation compared to other developed countries to deter or at least to suppress the terrorist activities in Indonesia, and the problems of tracing down the network of the terrorist movement after the closing down all of related virtual network of terrorist as the hydra effect.

A combination of persuasive approach to young generation and the Deterrent approach by detachment 88 are currently performed by Indonesian government. With the detachment 88 a military approach is recognized as shock therapy intended to deter individual terrorist and terrorist organization to conduct their terrors on individuals and to the state in general. Persuasive approach is conducted with an educative method, persuading young men to use cyber media appropriately, to increase their cyber awareness, to introduce some positive and productive aspects of cyber media, and to establish groups of cyber literate young Indonesian. An institutionalized approach is involving the state in programming the reinforcement of the basic values of "Pancasila" unifying all Tribes, Religious followers, race, and customs live in harmony under the umbrella of Pancasila.

References

Andieny, Ct. "Cyber Crime in Indonesia" reported March 26, 2012, in website http://aca-andiartha.blogspot.co.id/2012/03/cyber-crime-di-indonesia-cybercrime.html.

NATO conference conducted in Ankara Turkey from 5-9 May 2014,

Indonesia's Cyber Counterterrorism: Innovation Opportunities for CT Policing, Published by RSIS (Rajaratnam School of International Studies), NTU, in January 2014,

SB. Agus, (2015), Deradikalisasi Dunia Maya: Mencegah SimbiosisTerorismedan Media' Penerbit Daulat Press, Jakarta.

Raffaele, Robert. (2006), A reported on an open block of news paper article of US Fed News Service, including US State News on 23 August 2006.

Voa News: (2006), Indonesian Police Charge Two Suspects with Cyber-Terrorism Open: block: newspaper Article Open: block: school Univ Authors Close: block: school Univ Authors Open: block: publication Block US Fed News Service, Including US State News Close: block: publication Block [Washington, D.C] 23 Aug

Kassim, Yang Razali. S.Rajaratnam School of International Studies, NTU. RSISPublication@ntu.edu.sg or call (+65) 6790 6982 to speak to the Editor RSIS Commentaries,. SIS COMMENTARIES (7)

JENNIFER ,YANG HUI. (Centre of Excellence for National Security, S. Rajaratnam School of International Studies Nanyang Technological University, Singapore.

Studies in Conflict & Terrorism, 33:171–191, 2010, Copyright © Taylor & Francis Group, LLC, ISSN: 1057-610X print / 1521-0731 online, DOI: 10.1080/10576100903400605.

http://www.thejakartapost.com/news/2015/12/10/indonesia-joins-world-fight-cyber-terrorism.html#sthash.CEXk8NA3.dpuf

http://www.thejakartapost.com/news/2015/12/10/indonesia-joins-world-fight-cyber-terrorism.html#sthash.CEXk8NA3.dpuf

Series in Machine Perception and Artificial Intelligence - Vol. 65