INDONESIAN INTERNET USERS POTENTIAL IN COUNTER-CYBER RADICALIZATION

POTENSI PENGGUNA INTERNET INDONESIA DALAM COUNTER-CYBER RADICALIZATION

Rizky Reza Lubis[1]
Univesrsitas Pertahanan Indonesia
(rizkyrezalubis@gmail.com)

Abstrak – Tulisan ini menjelaskan proses radikalisasi yang terjadi di dunia maya, dengan melihat bagaimana dan mengapa masyarakat Indonesia rentan menjadi target organisasi teroris khususnya dalam hal perekrutan melalui dunia maya. Teroris tidak hanya memanfaatkan akses internet sebagai sarana komunikasi, tetapi juga memanfaatkannya sebagai sarana dalam menyembunyikan identitas dan lokasi saat menyebarkan ideologi radikal. Konsep yang digunakan dalam tulisan ini adalah *cyber radicalization*, yang merupakan konsep baru yang terbentuk dari konsep ancaman *cyber* dan radikalisasi. Adapun hasil dari tulisan ini menunjukkan bahwa pengguna internet Indonesia memliliki potensi yang besar untuk melawan radikaslisasi di dunia maya dan memilki kapasitas dalam mendukung agenda *counter terrorism* di dunia maya. Namun, hal tersebut masih menghadapi beberapa tantangan, sehingga diperlukan pemanfaatan pengguna internet oleh pemerintah secara maksimum dalam agenda *counter-cyber radicalization.*

Kata Kunci: *Cyber*, radikalisasi, terorisme, Indonesia

***Abstract** - This paper discusses the process of radicalization in cyberspace. It will look at how and why Indonesia are vulnerable in society and targeted by terrorist organizations in an attempt to recruit them, especially in cyberspace. The terrorists have become expert, not only using the latest tools of internet communications, but to do it in a way that can shield their identities and even their locations when spreading the radical ideology. The concept that used in this paper is cyber-radicalization, which is the new concept that merged from cyber threat and radicalization. The result from this paper shown that Indonesia netizens (internet users) had great potency to fight radicalization in the cyberspace and the capacity for supporting government counter-cyber radicalization agenda. However, fighting cyber radicalization in that way faced several challenges. Therefore Indonesia's government should benefited the netizens to reach the optimum point on counter-cyber radicalization agenda.*

***Keywords:** cyber, radicalization, terrorism, Indonesia.*

[1] Alumni Universitas Pertahanan Indonesia, Program Studi Diplomasi Pertahanan Cohort 2.

Preface

Initially the Internet was created to facilitate communication between the academic and military circles connected in the network of The Advanced Research Projects Agency Network (ARPANET) in 1969.[2] Along with the development of Technology and Information (ICT), the internet can be used freely as a public service to communicate. However, it also experienced a shift in function, the Internet is also used as a medium in committing criminal acts, one of which is acts of terrorism. Terror acts carried out with internet related instruments are known as cyber terrorism acts. Cyber terrorism poses a threat to state defense and security because it is capable of destruction, alteration, and acquisition and retransmission to real objects and cyber networks.[3]

According to Dorothy E. Denning, the phrase cyber terrorism was first created in 1982 by Barry Collin who emphasized his definition of the situation when the physical world and cyberspace collide[4], then when a crime or act of terror occurs in the situation it is later called as cyber terrorism.[5] Collin asserted that in future cyber warfare will involve terrorists who use cyberspace to carry out their attacks on critical infrastructure. With the rapid development of technology today, it is possible to perform an attack through a single push of a button on the computer to damage and blow up infrastructure resulting in casualties, material loss and disruptive impact on state stability.[6] Relevant to the process of establishing and running an organization of terrorism, which tend to closely related to the development of technology, especially the Internet. There has been a great deal of terrorist crime within cyberspace, its starting point in 1998 in which half of the thirty terrorist organizations set by the U.S Antiterrorism and Effective Death Penalty Act of 1996 used the website to commit acts of terrorism.[7]

The use of cyberspace in acts of terror is a real and new threat to some

[2] Petrus Reinhard Golose, *Seputar Kejahatan Hacking: Teori dan Studi Kasus*, (Jakarta: Yayasan Pengembangan Kajian Kepolisian Indonesia, 2008).

[3] Dorothy E. Denning, *Terror's Web: How the Internet Is Transforming Terrorism, Handbook on Internet Crime*, (New York: Willan Publishing, 2009).

[4] The word cyberspace often used as *cyber world* which means being in the realm of cyberspace.

[5] Dorothy E. Denning, Loc., Cit., hlm. 194-212

[6] Clay Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", *Focus on Terrorism*, Vol. 9, 2003, hlm. 1-42.

[7] Petrus Reinhard Golose, Invasi terorisme ke cyberspace. (Jakarta: YPKIK/Yayasan Pengembangan Kajian Ilmu Kepolisian, 2015).

countries.[8] The worst scenario is when a country will not only take steps that have been controlled by the majority of countries, that is the traditional approach; Military facing military or state facing the country. But the enemy will have an unprecedented new pattern, including the utilization of non-state actors that trigger asymmetric warfare, one of which is the use of terrorist groups.[9] Terrorists performing their action on cyberspace and get support from a country will be a global threat. Countries that benefit from this context are countries that have superior technological capabilities (predominantly developed countries) and are willing to seriously exploit the potential of cyberspace as an element of state defense and security.[10]

Interestingly, in addition to committing acts of terror, terrorist networks utilize cyberspace as a medium in spreading radical or radicalisation. Despite the many positive things of the Internet, the internet with all the features and freedom of access (especially in democracies) provides opportunities to occur or at least support radicalization effectively and efficiently. The opportunity referred to the research of Von Bher, Anais Reding, and Edward Gribbon on "radicalization in the digital age" elaborated with the author's analysis, as follows:[11]

1. Internet connecting people without knowing the territorial borders of the country opens the opportunity to disseminate and instill ideology and radical understanding to all internet users in the world.
2. Internet as "echo-chamber", where the internet provides easy access to obtain various information, including information about terrorism. The information obtained will continue to grow and spread to other media.
3. The Internet becomes an accelerator of radicalization. Internet users who have an

[8] James Andrew Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, (Washington, DC: Center for Strategic & International Studies, 2002).

[9] David J. Kilcullen, *Three Pillars of Counterinsurgency.* Pidato pada *the U.S Government Counterinsurgency Conference*, (Washington D.C, 28 September 2006).

[10] James Andrew Lewis, Op.cit. hlm 4.

[11] Von Bher et. al., *Radicalization in the Digital Era*, (Santa Monica: RAND Corporation, 2013).

4. understanding that leads to radical and extreme ideology tend to get the courage to join the terrorist network after obtaining radical material on the internet.
5. The Internet provides higher security guarantees than radicalization in the real world. Given the teaching of radical ideology can be done without having to meet directly. This will guarantee confidentiality of identity and location.

With all the advantages provided by the internet in the context of radicalization in cyberspace, the government's handling also needs to be in cyberspace. Interestingly, for democracies that have the demand to guarantee freedom of expression and association suffer a dilemma when implementing counter-cyber radicalization programs or counter-radicalization efforts in cyberspace. The country can not brutally block the websites and social media because it would violate some of its citizens' rights. In addition, the assessment of "terrorists" and "radicals" is the subjectivity of its judges. So the process of filtering web sites and social media accounts are very selective. The government needs a creative way of counter-cyber radicalization without violating the rights of its citizens.

Cyber Radicalization

Before going further in discussing radicalism in cyberspace, basically radicalization needs to be understood not as a form of dissemination of terror, but as a "process" in developing extremist ideology and belief. Referring to the Oxford Dictionary, Radicalization is an act or process that causes individuals to be in a radical position in political and social issues. This is in line with the definition of radicalization of Wilner and Dubouloz:[12]

> *"Radicalization is a personal process in which individuals adopt extreme political, social, and/or religious ideals and aspirations, and where the attainment of particular goals justifies the use of indiscriminate violence. It is both a mental and emotional process that prepares and motivates an individual to pursue violent behavior".*

Thus, from this definition it can be understood that radicalization as a

[12] Alex S. Wilner dan Claire-Jehanne Dubouloz, Homegrown terrorism and transformative learning: an interdisciplinary approach to understanding radicalization", *Global Change, Peace & Security*, Vol. 22, No. 1, 2010, hlm. 33-51.

"process" in making individuals adopt radical thinking that has consequences for acts of terrorism and extremism. Along with the development of technology, radicalization or how to spread radical understanding also experiences the development of cyberspace, as mentioned earlier, namely cyber radicalization. Here are the phases of radicalization along with the development of technology:[13]

- Phase 1: In 1984, radicalization began with sermons / lectures, printed newspapers / magazines, and video tapes of lectures or "struggles" by force.
- Phase 2: The mid-1990s, internet sites, such as Al-Neda and Azzam Publications.
- Phase 3: Mid 2000s, interactive forum on cyberspace. At that time began to emerge online forums of discussion on extremist ideology and belief.
- Phase 4: late 2000s; the spread of radicalism into the realm of social media along with the increase of social media users. The social media that is often used is Facebook, Youtube and Twitter.

Radicalization in cyberspace will continue as radical dissemination and propaganda will be more effective and efficient when done in cyberspace. Cyber radicalization will create opportunities for self-radicalization, in which individuals become terrorists without direct affiliation with radical groups but they still gain influence from the ideology and message of the terrorists, commonly called "lone wolf" terrorists,.[14]

Although not moving in groups, terrorists created from self-radicalization are a serious threat. There is a tendency for massively moving terrorist groups to get help from those who do self-radicalization and even they come to the group to propose themselves as members. This can be seen from the case of Mohammed Atta and three others directly involved in the 9/11 attacks, withdrawing them, themselves domiciled in Hamburg, Germany which

[13] Aaron Y. Zelin, Richard Borow Fellow, "The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis", Washington Institute for Near East Policy, January 2013.

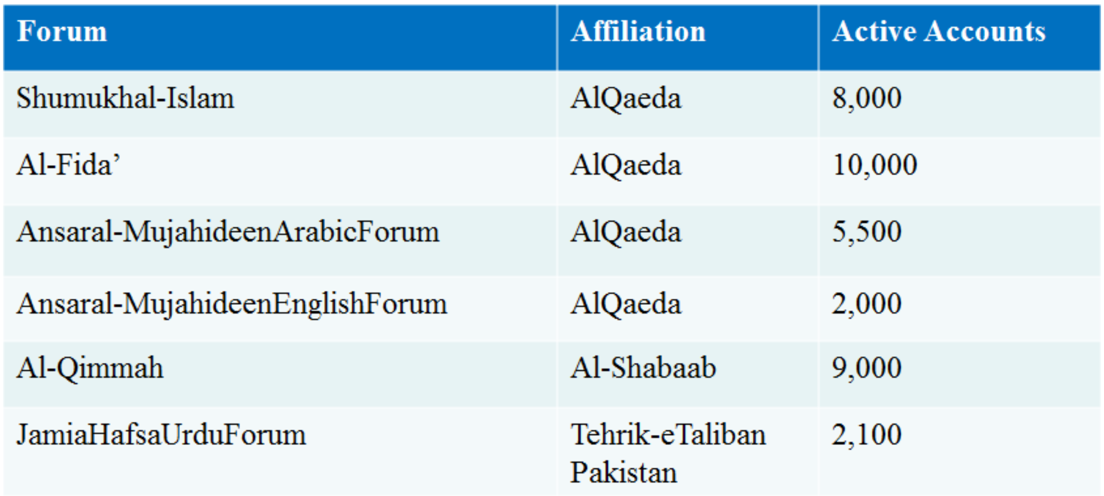
[14] "Self-Radicalization", Citizendium, dalam http://en.citizendium.org/wiki/Self-radicalization, 23 September 2013, diakses pada 2 Juni 2017.

then traveled to Pakistan. Then another case in London suicide bombings in 2005 conducted by terrorists who are British citizens themselves. The results of the investigation indicate that the terrorists gain an understanding of the internet and then visit Al-Qaeda to get training that culminates in a "Jihad" action in their own country.[15]

As for cyber radicalization has a variety of forms, at the stage ofpromoting the ideology or understanding of terrorist groups, they tend to use social media with links leading to websites or online forums that provide more detailed information than social media that is too open to the public. The websites or online forums are diverse and numerous in shape, and tend to have the following features;[16]

- Contains persuasive content in justifying terrorist beliefs and ideologies and affirming the errors of other ideological beliefs, including the ideology of secular states.
- There are photo news, and videos that show suffering and oppression to raise sympathy, but there are also those who show extremist "action".
- Having two or more language versions, it shows the target of cyber radicalization is a global society.
- Specifically for members / passwords (password-protected) in order to enter and view the content of the website. This is done as a form of anticipation of

Table 1. Radical Online Sites and Forums



Forum	Affiliation	Active Accounts
Shumukhal-Islam	AlQaeda	8,000
Al-Fida’	AlQaeda	10,000
Ansaral-MujahideenArabicForum	AlQaeda	5,500
Ansaral-MujahideenEnglishForum	AlQaeda	2,000
Al-Qimmah	Al-Shabaab	9,000
JamiaHafsaUrduForum	Tehrik-eTaliban Pakistan	2,100

Source: Anton Ali Abas, Presentation in Media and Terrorism Course, Asymmetric War Studies Program, Indonesian Defense University October 13, 2015.

[15] Bruce Hoffman, *Challenges for the U.S. Special Operations Command posted by the Global Terrorist Threat: al-Qaeda on the Run or on the March?*, (George Washington D.C: Middle East Policy, 2013).

[16] Anton Ali Abas, Paparan Mata Kuliah Media dan Terorisme, Program Studi Peperangan Asimetris, Universitas Pertahanan Indonesia, 13 Oktober 2015.

terrorist organizations so as not to be seen by the government or cyber police. Although, cyber police will be very easy to check the contents of online discussion forums that use a password or private but if not open to the public, it is likelyhood to be known by cyber police will be smaller.

Use of websites and online discussion forums is an effective option in recruiting and gathering sympathy. This can be seen from the number of members of the closed online groups. These are the most famous international discussion forums and have many active members:

In promoting these websites and online discussion forums terrorist groups tend to use social media. In addition, social media is understood as a fairly relevant and effective instrument in cyber radicalization. One example is the recruitment of jihadist candidates through Facebook to be sent to Syria in 2014, among them citizens who have been deported from Turkey and examined as witnesses. According to his statement, they will leave for Syria by gaining access from friends on Facebook. Initially, the witness received a friendship invitation on Facebook with an unknown person, the witness accepted the friendship because it saw the writings on the Facebook page is very Islamic and tell a lot about daulah or ISIS power in Syria. Friendship on Facebook continues with the use of a personal chat facility which in turn gets an offer to go to Syria.[17]

The example shows one form in promoting radical ideology and garnering support through social media. Social media is the most frequently used are social media with the most demands, where the top three are Facebook, Youtube and Twitter. The character of social media accounts in the context of radicalization can be seen in the following table:

[17] Petrus Reinhard Golose, *op.cit.*

Table 2. Social Media Used as Cyber Radicalization Instrument

Facebook	*Multiple accounts* *Private Messaging and Chat* *Closed groups*
YouTube	*Media dissemination* *Validation* *Messaging*
Twitter	*Wide broadcast* *Multiple accounts* *Direct Messaging*

Source: Anton Ali Abas, Exposure to Media and Terrorism Courses, Asymmetric War Studies Program, Indonesian Defense University, October 13th, 2015.

Related to the use of social media whose main function is to share videos, such as Youtube, cyber-radicalization is done by spreading the specifically themed video. There are six categories of themes that are usually uploaded to the internet by terrorist groups:[18]

1. Operational Video (at the time of their assault).
2. *Hostage Video*
3. Videos that provide statements representing their groups.
4. *Tribute Video.*
5. *Internal Training Video*
6. Videos that give instructions to the public.

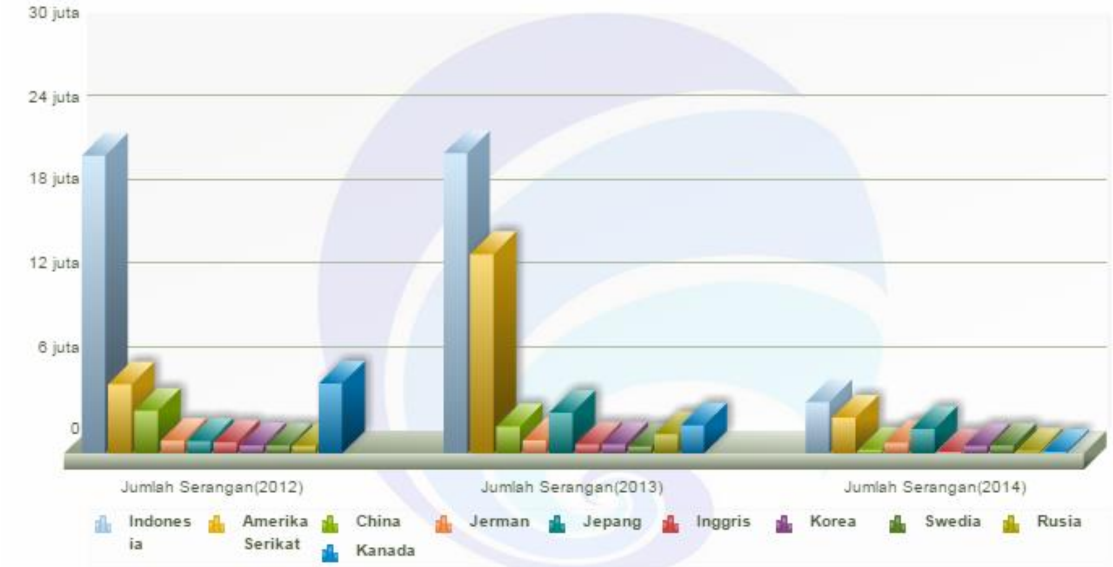
Cyber-radicalization through social media is a matter to watch out for because it is most easily spread and popular. In addition, the majority of users are teenagers who do not have the mental establishment so vulnerable to be a target of radicalization. Although cyber-radicalization (as well as all other terrorism-related matters) tends to be indiscriminate against its target.

Cyber Radicalization **in Indonesia**

Since the collapse of the World Trade Center (WTC) in September 2011 and in particular on the Bali Bomb I event, Indonesia has been paying serious attention to the issue of terrorism and actively participating in the "war on terror" policy launched by the United States. But this becomes a dilemma of its own. For countries that are still facing unemployment and poverty problems such as Indonesia, it will be even more complicated to choose what comes first between tackling economic problems or tackling terrorism. Not to mention for the majority Muslim countries, often the government has to deal with its own community. Basically not all Muslims in Indonesia have radical understanding and lead to the terrorist movement, but based on the diversity of religion in Indonesia, terrorist acts are often done

[18] Anton Ali Abas, *op.cit.*

Graph 1. Countries Targeted by Cyberattack and Cyberterror in 2012-2014



Source: Ministry of Communications and Informatics, 2017, Data and Statistics; Cyber Security and Governance, in https://statistik.kominfo.go.id/site/searchKonten?iddoc=1370, accessed on 2nd June 2017.

by the party who claims that he is a Muslim and it is a risk for majority religion.[19] It is this kind of dilemma that sometimes triggers domestic tensions that can trigger the disintegration of the nation. Under these conditions, it can be understood that terrorism has become a real threat to Indonesia.[20]

Indonesia is a country vulnerable to the threat of terrorism, this can be seen from the many acts of terror in Indonesia, as in the big cases: Bali Bomb I in October 2002, Bali Bomb II in October 2005, JW Marriot Hotel and Hotel Ritz Calton in July 2009, the AustralianEmbassy in September 2004.[21]

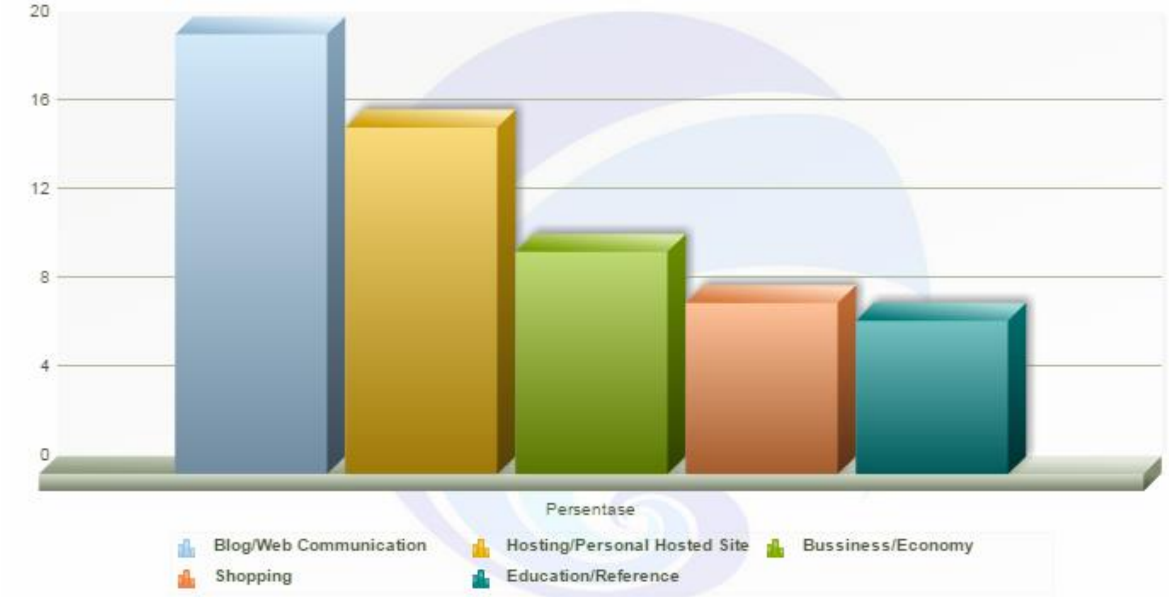
Plaza Sarinah in January 2016, to the Kampung Melayu Terminal in May 2017. In addition, there is also the involvement of Indonesian citizens in international terrorist networks such as ISIS, Al-Qaeda, Jamaah Islamiyah,

[19] "Terorisme Dikaitkan Islam, BNPT: Itu Resiko Agama Mayoritas", Republika, 15 April 2016, dalam http://nasional.republika.co.id/berita/nasional/umum/16/04/15/o5neyu377-terorisme-dikaitkan-islam-bnpt-itu-resiko-agama-mayoritas, diakses pada 17 Juli 2017.

[20] "Terorisme masih jadi ancaman nyata tahun 2016", Rappler, 29 Desember 2015, dalam http://www.rappler.com/indonesia/117434-terorisme-masih-jadi-ancaman-nyata-tahun-2016, diakses pada 13 Agustus 2016.

[21] Jeneman Iskandar, "Perubahan Pola Serangan Teorisme di Indonesia: Studi Kasus Tahun 2000-2013", (Jakarta: Dapur Buku, 2014).

Graph 2. Category of Malicious Websites in Indonesia



Source: Ministry of Communications and Informatics, 2017, Data and Statistics; Cyber Security and Governance, in https://statistik.kominfo.go.id/site/searchKonten?iddoc=1370, accessed on 2nd June 2017.

Abu Sayyaf and so on.[22] As for the threat of terror that occurred in cyberspace, referring to the statistical data of the Ministry of Communications and Informatics, Indonesia occupy the top position of vulnerability in cyber attacks. This makes Indonesia often a target of attacks on cyberspace when compared with other countries. As illustrated in the graph.

One of the cases of terrorism with the use of cyberspace in Indonesia that received the spotlight is the case of Imam Samudra, a convicted individual who died on the Bali Bomb case. At that time, Imam Samudra could control the terrorist network from his prison cell using the internet.[23] In addition, the most frequent threat in cyberspace in Indonesia is the use of internet sites in conducting propaganda and brain washing to spread radical ideology or commonly called cyber radicalization.[24]

The Indonesian government itself in assessing some cases of internet use as a media of cyber radicalization is still subjective, whether the action leads to terror acts or not. As for the case which clearly states cyber radicalization and

[22] Golose, *op.cit.*

[23] Imam Samudra managed to smuggle the laptop into the cell with the help of a Kerobokan Prison Guard, who had previously been recruited as terrorist member in prison. Based on the International Growth Center Report in Peter Reinhard Golose, Invasion of Terrorism to Cyberspace. (Jakarta: YPKIK/Yayasan Pengembangan Kajian Ilmu Kepolisian, 2015), hlm. 18-19.

[24] Von Bher, *op.cit.*

continued with terror in Indonesia is Al-Kitabatul Maut Al Alamiya website or the international death brigade which claimed responsibility in Bali Bomb I case in 2002.[25] In addition, there is a case called Santoso who leads the network of the East Indonesian Mujahidin Group who expressed their support for ISIS leader Abu Bakar Al Bahgdadi through a video on YouTube. The action ended with a number of Indonesians who claimed to be in ISIS, Iraq and Syria, and invited the public to join the jihad with ISIS in the country.[26]

As a precaution against the recurrence of such acts of terror and radicalization and restricting the movement of terrorist networks in Indonesian cyberspace, the Indonesian government with the legitimacy granted to the National Agency for the Control of Terrorism (BNPT) has blocked sites considered to spread radical and extreme insights. Here's a list of eleven popular sites and getting blocked:[27]

1. voa-islam.com
2. nahimunkar.com
3. kiblat.net
4. bisyarah.com
5. dakwahtangerang.com
6. islampos.com
7. suaranews.com
8. izzamedia.com
9. gensyiah.com
10. muqawamah.com
11. abuzubair.net.

In addition, BNPT has also blocked several personal sites like blogspot and wordpress that have radical content. The challenge faced is the large number of private sites users in Indonesia (see Graph 2), thus made this blocking approach take considerable time, considering when the site is blocked or deleted by the government, new sites will appear because the site is unpaid and new or double account creation procedures can be done easily.

[25] "We Bombed Bali", dalam http://www.theage.com.au/articles/2002/12/12/1039656175179.html, 13 Desember 2002, diakses pada 6 Juni 2017.

[26] "ISIS Sebar Pemahaman Radikal melalui Media Digital", dalam http://www.bbc.com/indonesia/berita_indonesia/2015/03/150301_radikalisme_anakmuda_sosmed, 2 Maret 2015, diakses pada 6 Juni 2017.

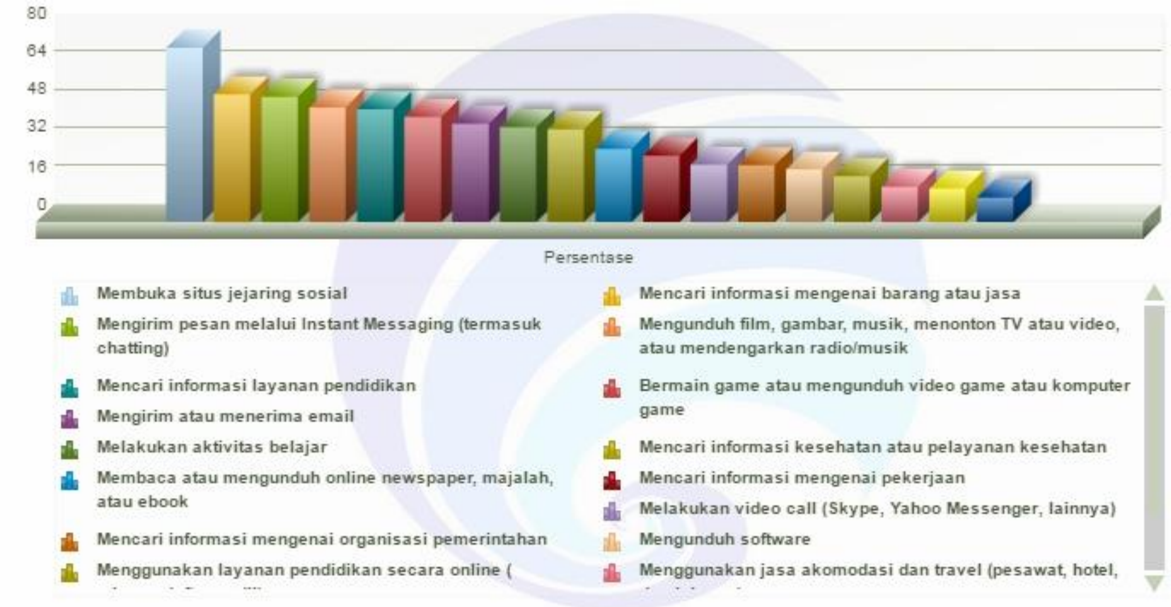
[27] "11 Situs terbaru yang diblokir pemerintah", dalam http://megapolitan.kompas.com/read/2017/01/04/10150067/ini.dia.11.situs.yang.terbaru.diblokir.pemerintah, 1 April 2017, diakses pada 6 Juni 2017.

Indonesian Potential Internet Users in Counter-Cyber Radicalization

Cyber radicalization is different from conventional radicalization (which takes place in the real world), a special approach is needed in the realm of cyberspace. Governments can easily block or delete sites, personal blogs, and social media accounts that are considered to have radical content. The problem is the site and social media will continue to exist and regenerate with new accounts. In addition, brutal blocking and removal will create a negative value for a democratic country that supports freedom of expression.

In this context, the focused model of handling is counter-cyber radicalization which departs from the concept of cyber security and counter-radicalization. Counter radicalization is essentially an effort other than de-radicalization in preventing the growing extremist tendencies in society. If wisely implemented counter-radicalization will be more effective than de-radicalization because counter-radicalization is an opposition to the process of spreading

Graph 3. Internet User's Activity by Individuals in Indonesia



Source: Ministry of Communications and Informatics, 2017, Data and Statistics; Cyber Security and Governance (Ditjen PPI), available at https://statistik.kominfo.go.id/site/searchKonten?iddoc=1370, accessed on 2nd June 2017.

radical ideas and focuses on embryonic radicaliasation, whereas de-radicalization focuses on changing the radical (back to normal).[28]

Utilization of cyberspace insturments, especially in the context of social media to counter-radicalization can be categorized as counter-cyber radicalization. Counter-cyber radicalization needs to be done because today more and more terrorists are in the virtual world in the dissemination of massages, hostile propaganda and the promotion of acts of violence. Some findings of cyberspace use by terrorist group in Indonesia that cyberspace is used to release manifestos, propaganda and agitative statements, garner support and network strengthening, communicate between networks and recruit new member.[29]

According to the authors' note, there are some potential Indonesian internet users to counteract or become part of a counter-radicalization agenda that is not only on normative ground, but focuses on embryo radicaliation in the cyberspace. Firstly, the large number of

internet users in Indonesia and tendencies to be very active in social media makes Indonesia easy to raise something into viral issues only with capitalize the hashtags.[30] *Cyber-radicalization done through social media will be ineffective if the majority of social media users participate in disseminating content that contradicts radical ideology*. Thus the taks of the government is to release content (which is propaganda) and campaign to counter radicalization on the internet, the most effective is to

use hashtag. Internet users who capture the massage are likely to spread the content and make it a trend. According to the author, of many contexts in cyberspace, social media is the most important thing to

[28] Farhan Zahid, "Analyzing the Counter-Radicalization and De-Radicalization Models" dalam http://www.cf2r.org/fr/foreign-analyzes/analyzing-the-counter-radicalization-and-de-radicalization-models.php, 13 Desember 2016, diakses 19 Juli 2017.

[29] Petrus Reinhard Golose, *op.cit.*

[30] Hashtag is a spaceless word or phrase beginning with a hash symbol ("#"). Hashtags used to classify specific themes or topics in social media, and on the other hand hashtags also make it easier for others to find related topics. See, "Definisi Hashtag pada Sosial Media", in http://organix-digital.com/blog/read/definisi-dan-fungsi-hashtag-pada-sosial-media, 11 April 2014, diakses pada 3 Juni 2017.

note as and issue tends to be popular and spread quickly through social media. Moreover, the use of internet in

Secondly, the Indonesian Society is able to produce joke products very quickly and make it popular with a matter of minutes in cybersapce. The humor of Indonesian society has been recognized by the world community. This is evident from the Bomb case in the Sarinah Thamrin area on January 14th, 2016, after the incident in a matter of minutes the trend in the social media world immediately turned into the issue of the bombing. Interestingly, unlike the case of terrorism in Paris, France[31], the majority of Indonesian (especially Jakarta) responses in social media do not show the fear of terror; It makes the act of terrorism a matter of joke and satire against radical ideologies. This is indicated by the large number of meme productions (pictures with writing) and the social status of the media that are satirical. At that time, the response of internet users in Indonesia became a symbol that terrorism does not make the Indonesian people fear that is marked by

Indonesia is dominated for social media purposes, as illustrated in the last graph.

hastag "#KamiTidakTakut" that spread throughout the world. It shows that acts of terrorism aimed at spreading terror and fear have failed or can be denied by the response of Indonesian internet users.[32]

In addition, in the case of the Kampung Melayu Terminal bombing in May 2017, the "#KamiTidakTakut" hastag became a world trend. This is a simultaneous response of Indonesian internet users without any party coordination. Therefore, if the government is able to exploit these potentials by making it part of the counter-cyber radicalization agenda then this will be the most efficient and effective way. Because after all the atmosphere of terror and public opinion created can only be controlled by the public itself. Technically the government can utilize well-known public figures and is active in cyberspace as an agent in controlling public opinion. Status on facebook, Twitter chirp and Youtube

[31] "Paris Massacre: At least 128 die in attacks", dalam http://edition.cnn.com/2015/11/13/world/paris-shooting/index.html, 14 November 2015, diakses pada 4 Juni 2017.

[32] Rizky Reza Lubis, "Fight Radicalization with 'Ridicoulization'", Essay for FPCI International Internship Program 2016 on Germany, Theme: The Role of Young Generation in Counter Terrorism, FPCI.

Videos by the characters tend to be more quickly accepted and spread in cyberspace.

The engagement of Indonesian internet users on the counter-cyber radicalization agenda will have an impact on two phases; First, when cyber radicalization takes place where internet users who are part of the agenda will counter radical ideology and understanding by turning them into jokes that ultimately make the ideology and understanding unpopular. Second, in the event of acts of terror such as bombing and suicide bombing. Such terror acts will have the effect of fear and panic which are the main objectives of terrorists; which is also considered a terrorist success in conveying the message to the next "terrorist" candidate. But with so many social media accounts opposing and portraying such acts as silly acts then it will show terrorists in the delivery of their messages through the act of failed terrorism.

Counter-Cyber Radicalization Challenge in Indonesia

Indonesia with its potential internet users in counter-cyber radicalization has three challenges to be considered: first, the lack of public awareness of "terrorism" matters. If people are able to change popular culture that radicalism and acts of terror are a joke so that the enthusiasts or victims of radicalization will decline, the consequence will be to reduce the awareness that has been awakened by a sense of "fear" of acts of terrorism. However, the lack of radical interest in cyberspace does not mean stopping the action of terrorist networks. This makes counter-radicalization efforts through the utilization of internet users in cyberspace effective but will create a new blind spot. The government should be able to close the blindspot by continuing to give continuous appeals without causing panic and fear.

Second, discredit certain groups. Giving public opinion to assume an ideology or understanding is radical and extreme has the consequence of discrediting and creating stereotypes in society with groups (in this context of religious teachings) which are the basic logic of the terror act. As in Indonesia, the majority of terrorists claim to be

Muslims, though not in accordance with the original teachings of Islam, but this will lead to public opinion that the basic or pure religion that the terrorist claims is part of the joke. This has the potential to become one of the disintegrating factors of the nation.

Conclusion

Cyber radicalization is a real threat to a country and Indonesia is one of the most potential countries to be a target of terrorists and radicalization (including its cyberspace). Attempts to deal with radicalization in cyberspace will not be as effective as handling it in the real world. Moreover, Indonesia is a democratic country that keeps the freedom of expression of its people, so it can not arbitrarily block social media sites and accounts.

Creative and effective ways are needed in counter-cyber radicalization, one of which is to utilize the potential of Indonesian people who use the internet. Many Indonesian internet users and creatively able to raise a viral issue to be used as counter-cyber radicalization agenda in controlling public opinion that radical understanding is a negative thing. In addition, when an act of terror internet users by itself will fight the panic and fear generated with the social media. It will reduce radical ideology enthusiasts. But in practice, the government should pay attention to the level of "awareness" of the community and the position of a particular religion in order not to be discredited, given the number of campaigns in cyberspace that oppose radicalism.

References

Book

Denning, Dorothy E. 2009. *Terror's Web: How the Internet Is Transforming Terrorism, Handbook on Internet Crime.* New York: Willan Publishing.

Golose, Petrus R. 2008. *Seputar Kejahatan Hacking: Teori dan Studi Kasus*. Jakarta: Yayasan Pengembangan Kajian Kepolisian Indonesia.

Golose, Petrus R. 2015. *Invasi Terorisme ke Cyberspace*. Jakarta : Yayasan Pengembangan Kajian Ilmu Kepolisian.

Hoffman, Bruce. 2013. *Challenges for the U.S. Special Operations Command posted by the Global Terrorist Threat: Al-Qaeda on the Run or On the March?* George Washington D.C.: Middle East Policy.

Iskandar, Jeneman. 2014. *Perubahan Pola Serangan Teorisme di Indonesia: Studi Kasus Tahun 2000-2013*. Jakarta: Dapur Buku.

Lewis, James A. 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC: Center for Strategic & International Studies.

Stein, Ruth. 2010. *For Love of the Father: A Psychoanalytic Study of Religious Terrorism.* Stanford: Stanford University Press.

Von Bher et. al. 2013. *Radicalization in the Digital Era*, Santa Monica: RAND Corporation.

Zelin, Aaron Y dan Richard Borow Fellow. 2013. *The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis.* Washington : Washington Institute for Near East Policy.

Journal

Jackson, Richard. 2007. *Constructing Enemies: 'Islamic terrorism' in political and academic discourse.* Government and Opposition. Vol. 42. No. 3.

Wilner, Alex S. dan Claire-Jehanne Dubouloz. 2010. "Homegrown terrorism and transformative learning: an interdisciplinary approach to understanding radicalization". *Global Change, Peace & Security*. Vol. 22 No. 1.

Wilson, Clay. 2003. *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. Focus on Terrorism*. Vol. 9.

Website

"ISIS Sebar Pemahaman Radikal melalui Media Digital", dalam http://www.bbc.com/indonesia/berita_indonesia/2015/03/150301_radikalisme_anakmuda_sosmed 2 Maret 2015, diakses pada 6 Juni 2017.

"*Self-Radicalization*", dalam http://en.citizendium.org/wiki/Self-radicalization, 23 September 2013, diakses pada 2 Juni 2017.

"Paris Massacre: At least 128 die in atta cks", dalam http://edition.cnn.com/2015/11/13/world/paris-shooting/index.html, 14 November 2015, diakses pada 4 Juni 2017.

"Definisi Hashtag pada Sosial Media", dalam http://organix-digital.com/blog/read/definisi-dan-fungsi-hashtag-pada-sosial-media, 11 April 2014, diakses pada 3 Juni 2017.

"Terorisme masih jadi ancaman nyata tahun 2016", dalam http://www.rappler.com/indonesia/117434-terorisme-masih-jadi-ancaman-nyata-tahun-2016 29 Desember 2015, diakses pada 13 Agustus 2016.

"We Bombed Bali", dalam http://www.theage.com.au/articles/2002/12/12/1039656175179.html, 13 Desember 2002, diakses pada 6 Juni 2017.

"Situs terbaru yang diblokir pemerintah", dalam http://megapolitan.kompas.com/read/2017/01/04/10150067/ini.dia.11.situs.yang.terbaru.diblokir.pemerintah, 1 April 2017, diakses pada 6 Juni 2017.

"Radicalization", Oxford Dictionary dalam https://en.oxforddictionaries.com/definition/radicalization, 19 Juli 2017, diakses pada 19 Juli 2017

Farhan Zahid, "Analyzing the Counter-Radicalization and De-Radicalization Models" dalam http://www.cf2r.org/fr/foreign-analyzes/analyzing-the-counter-radicalization-and-de-radicalization-models.php, 13 Desember 2016, diakses pada 19 Juli 2017.

Others

Abas, Anton A. 13 Oktober 2015, Paparan Mata Kuliah Media dan Terorisme, Program Studi Peperangan Asimetris, Universitas Pertahanan Indonesia.

Lubis, Rizky Reza. 2016. “Fight Radicalization with “Ridiculization”. *Essay for FPCI International Internship Program 2016 on Germany. Theme: The Role of Young Generation in Counter Terrorism,* FPCI.

Kilcullen, David J. 28 September 2006. *Three Pillars of Counterinsurgency.* Pidato pada *the U.S Government Counterinsurgency Conference.* Washington D.C.