International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 9, Issue 10
October, 2022
Pages: 22-33

Cyber Cooperation between Indonesia and the United States in Addressing the Threat of Cyberterrorism in Indonesia

Bimo Arya Putra

Universitas Pembangunan Nasional Veteran Jakarta, Indonesia

http://dx.doi.org/10.18415/ijmmu.v9i10.4058

Abstract

The development of technology and the increasing use of the internet has increasingly made the dominance of the cyber world in all international issues inseparable. The cyber world itself is a relatively new concept, with very minimal international regulations on how a country should act in this domain. Realizing this, many countries in the world are starting to make many strategies and plans in capitalizing the cyber world for their benefit but some still need to survive. To deal with this, many countries have begun to cooperate in an effort to increase their capabilities in the massive cyber world, this not only provides many opportunities for development but also creates many new threats such as hacktivism, cyberspaces, cyberterrorism. With the urgency that exists, Indonesia has begun to initiate cooperation with various countries on cyber issues, including with the superior country the United States in the agreement regulated by the Letter of Intent (LoI). The author has identified cyberterrorism as one of the threats that needs to be analyzed due to its large threat to Indonesia. By examining the LoI, the author has concluded that being led by the National Cyber and Code Agency (BSSN), there are 2 important aspects in dealing with cyberterrorism, namely capacity building and information sharing. Although these two things have been done, the impact has not significantly developed Indonesia's cybersecurity due to the lack of intense and effective implementation of the two programs.

Keywords: *Cyber World; Cyber Cooperation; Indonesia and the United States; BSSN, Cyber Security; Capacity Building; Information Sharing; Cyberterrorism*

Introduction

Almost everything we do in everyday life depends on computers and computer networks. The Internet has become a critical infrastructure for governments, companies, and financial institutions. Society's increasing reliance on information and communication technology (ICT) at all levels has changed the way individuals interact today. The social activities of various peoples in the world at all levels connected to the internet are contained in the domain called cyberspace. With the continued development of technology, of course, this use will continue to develop. As a result of the rise of technology along with the increasing variety of its use, such as economic and political incentives to exploit networks with nefarious purposes have also increased, and cybersecurity has reached a level that the state pays great attention to (Todes, 2004).

The concept of a cybersecurity threat as a malicious act that seeks to damage, or steal data, and disrupt digital life in general. Cyber-based technology is now ubiquitous around the world. It is certain that criminals, terrorists, and spies also rely heavily on cyber-based technology to support their goals. These criminals can access cyber-based technologies to refuse service, steal or manipulate data, or use devices to launch attacks on themselves or other equipment. Examples of common cyber threats are cyberterrorists, cyberspaces, cyberthieves, cyberwarriors, and cyberActives (Obotivere & Nwaezeigwe, 2020).

Some cases of cyber threats in the world such as the Internet worm cyberattack that occurred after the occurrence of the 911 event, called Nimda, spread throughout the country in less than an hour and attacked 86,000 computers. These attacks raise public awareness about how vulnerable the system at the time was to cyber-terror cyberattacks could also cripple activities in vital life-sustaining sectors such as the economy (Kemmerer, 2016).

One of the largest cyber-attack events occurred in Estonia, In the spring of 2007 Estonia fell under a 22-day cyber-attack campaign targeting Estonia's internet-connected information systems. Where the wide-scale calculation of the availability of public digital services has a significant influence on the way of life of ordinary citizens and businesses (Ottis, 2008).

Indonesia has also experienced millions of cyber-attacks, even Indonesia is one of the main targets of cyberattacks in Asia. In 2009 Indonesia was also one of the targets of the Stuxnet virus attack which many cyber experts consider to be the most advanced cyber weapon today because it is able to attack certain targets. Cyberattacks, if directed at Indonesia's vital infrastructure, will not only cause program damage, malfunctions, but also have the potential to cause casualties (Setiyawan, 2019).

This has caused Cyberterrorism to present a challenge for the Indonesian government to play a significant role in countering terrorists who maneuver in cyberspace. The Government of Indonesia is currently in the stage of formulating policies, strategies for resilience and security of information systems in order to deal with cyber threats, for example the Government of Indonesia established the State Cyber and Password Agency (BSSN) through Presidential Regulation Number 53 of 2017. The establishment of this agency is an effort by the government to maintain Indonesia's cybersecurity as one of the Government's fields that needs to be encouraged and strengthened to increase national economic growth and realize national resilience. The agency implements cybersecurity effectively and efficiently by leveraging, developing, and consolidating all elements related to Indonesia's cybersecurity. (Setiyawan, 2019)

Indonesia's efforts in realizing and developing capabilities in this field will face several challenges, such as inadequate cyber law policies and regulations, very weak coordination and cooperation in the government and private sectors, governance and national cybersecurity organizations that have not synergized, there are no standard mechanisms and protection of vital infrastructure, vital information infrastructure that has not been integrated and limited quality and quantity of resources human beings especially in the field of cybersecurity (Zainal A, 2013).

The Director of National Intelligence (DNI) stated that cyber threats are the number 1 strategic threat in the United States to replace the terrorist threat that first appeared in the 911 incident. (Billo & Chang, 2004).

In February 2003, President Bush issued a policy in the form of a National Cyber Security Strategy that underscores three priorities: preventing attacks on America's vital infrastructure, reducing national vulnerability to cyberattacks and minimizing damage and recovery time from cyberattacks. (Chen, 2013).

In America, cybersecurity responsibilities are carried out by the Department of Homeland Security (DHS), the Department of Defense (DoD) and the Federal Bureau of Investigation (FBI). DHS is responsible for internal security. DHS has a National Cybersecurity Division tasked with working with public, private, and international agencies to secure cyberspace and American interests in cyberspace (DHS, 2021).

The second responsibility for cybersecurity in America is carried out by the Federal Bureau of Investigation (FBI). The FBI is a federal agency that acts as a domestic intelligence agency as well as a federal law enforcement officer. This agency is responsible for defending the country from all forms of crime, acts of terrorism, foreign intelligence, law enforcement, and protecting civil rights (FBI, 2021).

But it is undeniable that after all the explanations above we can see that cyber handling in Indonesia is very far when compared to what America is doing, such as starting from handling institutions, work mechanisms and up to the existing legal umbrella. America as a developed country and the one that first understood the importance of cybersecurity has a more up-to-date system than Indonesia as a developing country, so it is important for Indonesia to continue to reflect and try to learn what is implemented in America. Realizing this, the two countries, namely Indonesia and the United States, have each made their efforts in realizing security in cyberspace. Indonesia's mission to improve the quality of security in cyberspace can finally be carried out with the signing of an LoI containing cooperation with the United States in improving cyberspace security signed in 2018.

However, after the signing of the cooperation, from 2018 until now, namely 2022, which means that the cooperation has been established for 4 years. Looking at the facts that occurred during these 4 years, no significant major developments have occurred to Indonesia's cybersecurity which should be the goal of cooperation. Despite having collaborated to discuss cyberspace security with a large country such as the United States, Indonesia still has not been seen to have a significant increase in cybersecurity aspects due to the many cyber-attack problems experienced and seems quite underestimated in the aspect of cybersecurity. One of the most recent was the event where the site of the National Cyber and Code Agency (BSSN) was successfully hacked by a hacker from Brazil. Cyberattacks have escalated and cyber warfare is haunting global security. However, there is no framework or authority governing cyberspace that is now considered a state jurisdiction. With this, various things that have been conveyed above the author raises the question, namely "How is the Implementation of Cyberspace Cooperation Between Indonesia and the United States in Increasing Capacity to Handle Cyber Terrorism Threats in Indonesia?".

The purpose of this study is to analyze what has been implemented in the Cyberspace Cooperation Between Indonesia and the United States in Increasing Capacity to Handle the Threat of Cyberterrorism.

Research Method

The study is based on retrospective design. The study is based on data collected from the secondary nepali political material and observations over a long period of time. Experience is another data method collection in this study. It is not described in every detail of the ethnic region and the different forms and contents of autonomous culture-based states proposed by various political and ethnic organizations, but it is a bird's eye view on the matter.

Meanwhile, the object of research used in this study is cyberspace cooperation between Indonesia and the United States and about Cyberterrorism. With the data used is the splicing of primary data as well as secondary data. With data collection techniques derived from literature studies and direct interviews conducted by BSSN & Indonesian Ministry of Foreign Affairs. The analysis techniques used by researchers in this study used data reduction, data presentation, and drawing conclusions.

Cyber Cooperation between Indonesia and the United States in Facing the Threat of Cyberterrorism in Indonesia

Cybersecurity is becoming increasingly important to the economy, security, and social well-being of the United States and Indonesia. Improving the exchange of information between resources requires special attention from both countries. This requires an agreed framework to understand the risks and obligations. Other legal structures and procedures and regulations should encourage sharing and collaboration. No single public or private sector organization can solve all problems, and every country can learn from other countries. Since most of the country's critical economic and infrastructure assets are privately owned and operated, cybersecurity-related solutions will require significant public-private collaboration. These include citizen education, labor and management Despite statements from senior officials, many still don't make cybersecurity a priority. However, the peoples of both countries understand the need for counterterrorism and disaster preparedness, and cybersecurity may be relevant to this.

Indonesia and the U.S. are democracies. They have the potential for democratic partnerships that can develop and deepen relationships to address differences and divisions with a great sense of maturity and responsibility. Cooperation between Indonesia and the U.S. is critical to strengthening ties between governments. In addition, the leaders of government agencies have regularly met and got to know each other better. Indonesia's strategic relationship with the U.S. is built on common interests that refer to two things, namely security cooperation in terms of america's overall bilateral relationship with Indonesia and the improvement of cooperation between the two countries towards the development of a new security architecture for the Asia Pacific region with the US has opened up a lot of cooperation at that location. Especially after the whole situation with China. The dynamics of cyberspace between the United States and China from 2010–2015 and 2015–2018 show that the power struggle in cyberspace has also transformed from an indirect form to a more direct tension between the two countries. This trend was realized by the issuance of the US Department of Defense Summary of Cyber Strategy which contains a more direct approach to securing the cyberspace of the United States which is equivalent to protecting its cyber sovereignty terms in a Chinese perspective. Furthermore, China also finally announced the enactment of the Cybersecurity Law which was perceived by the US as a direct effort from the Chinese Government to censor cyber content. Moreover, the failure of the 2015 deal to reduce tensions between the two countries also resulted in broader implications from China and the US trying to persuade the world to accept their perspective on cyberspace as well as to legitimize their position in ongoing tensions. (Juned et al., 2022)

The political dimension of the US-China cyber power struggle is one of the bridges between real-world rivalry and cyber power struggles between the two countries. Furthermore, the political dimension is strongly influenced by the decline of power between China and the United States since the beginning of the 21st century. The political dimension of competition also reflects competition in other dimensions that end up being security and economic. In this connection, there are several layers in the US-China political dimension of their cyber power struggle. The US and China have contrasting political ideologies where the US liberal democratic system that provides freedom for its people is different from China's authoritarian political system. However, China's increase in strength especially in economic power poses more of a threat to the United States recently along with an increase in cyber significance. Because of this, the prospect of cooperation between the United States and Indonesia is a tool of the US in maintaining and countering China's influence in the Digital region which is considered dangerous. (Juned et al., 2022)

Indonesia's current foreign policy is important to see Indonesia as a democratic force. Cyber cooperation offers Indonesia the opportunity to expand future security cooperation with the US in entering into some non-military issues that have the potential to impact the national security of the two countries but cannot be resolved unilaterally due to transnational cause and effect. Indonesia's hope for

cyber cooperation is to become southeast Asia's largest digital economy by 2030, according to a report by Standard Chartered Bank. Cyber cooperation for Indonesia can be seen as a significant multiplier of political and military power for Indonesia's interests. This is due to the strong military capabilities of the US regional, the accessibility of adequate technology, advanced Western training and intelligence, and the improvement of relations with the United States as a superpower in the world. (Ariesta, 2019)

Indonesia is an important partner in the Indo-Pacific Region, and the U.S.-Indonesia relationship is increasingly important. Indonesia is the third largest democracy in the world, the largest Muslim-majority country, the seventh largest economy by purchasing power, and a leader in ASEAN. It has the largest marine biodiversity in the world and the second largest terrestrial biodiversity. Indonesia also borders the South China Sea, which has the world's busiest sea lanes with more than $5 trillion in cargo and as much as 50 percent of the world's oil tankers pass through the South China Sea each year. The United States was one of the first countries to establish diplomatic relations with Indonesia in 1949, after its independence from the Netherlands. Indonesia as a country that is still developing certainly needs qualified cooperation partners such as the United States, especially in terms of cybersecurity because the US is a country that has long paid attention to securing the cyber world and has understood what kind of impacts can be caused, especially with the phenomenon of cyberterrorism which makes it necessary to handle it. Cyberterrorism itself is not a new problem for both countries because both have had a dark history.

Cyberterrorism is a type of crime that is included in the Cyber Crime category because cyber crime can simply be interpreted as a type of crime committed by using the internet media as a tool to carry out acts of terror. Cyberterrorism in cyberspace is growing so rapidly with various patterns of crime interactions committed by everyone who intends to commit criminal acts in cyberspace. Legal facts show that there is abuse of the use of the internet by terrorists, as was the case in Indonesia by Imam Samudra, a death row inmate of the Bali bombings, with his role in controlling terrorist networks from prison cubicles by communicating via the internet. Imam Samudra managed to smuggle a laptop into his cell with the help of a kerobokan prison warden, Benny Irawan, who was successfully recruited as a terrorist member in the prison. Another evidence of misuse of internet sites in the spread of terrorism propaganda. Online media that is popular for spreading terrorism is arrahmah.com and it is known that there is the involvement of Muhammad Jibril who also holds the title of Princes of Jihad as founder and Chief Executive Officer (CEO). (Golose, 2015).

Terror is an activity which terror organizations do for political purposes and objectives. The purpose is to topple the existing government, to uphold the new government system and others. The existing terror organizations in Indonesia are totally related to Islamic radical nuances. It is definitely obvious in view of Indonesia as the country the largest Muslim population in the world. Moreover, Indonesia becomes source of terror organizations to grow and become the target of terror itself. As the country with the largest Muslim population in the world but no existence and application of Islam Sharia Laws as state laws and regulations, Indonesia becomes the target of terrorism actions. Finally, it is considered a conflict of religious ideology which has to be solved definitely. (Juned, 2017)

President Regulation on Counter-terrorism is a regulation that contains the National Action Plan for Countering Extremism in Indonesia and an effort from the government to tackle terrorism softly. It will also implement several coordinated with various parties, namely related ministries or institutions. This is done to mitigate criminal acts of terrorism and violent extremism. This is a complementary instrument to various laws and regulations related to terrorism. Some of the discussions included in it include action steps to counter extremism.These steps include coordination between institutions/ministries to prevent and overcome violent extremism that leads to terrorism. Encouraging ministries/institutions and civil society to participate and synergize in countering violent extremism lead to terrorism. Furthermore, it explains the capacity of human resources in preventing extremism and conducting

surveillance, early detection and early prevention of acts of extremism. Another discussion is about the attention and protection of victims of criminal acts of terrorism. (Juned et al., 2022)

Implementation of Cyber Cooperation in Cyberterrorism Handling by BSSN

National Cyber and Code Agency (BSSN), which is the most important vocal point or actor in cyber cooperation between Indonesia and the United States, of course, in the 4 years of cooperation from 2018 regulated in an LoI, has carried out various programs to realize what is the purpose of this cooperation began, it is important to understand what kind of performance has been done and how much results have been obtained in order to fully understand the significance of this cooperation to the development of cybersecurity in Indonesian.

At the bilateral level, Indonesia currently has a Memorandum of Understanding (MoU) or Letter of Intent (LoI) on cybersecurity or cyber cooperation with 10 countries, namely the United States, The United Kingdom, Russia, China, Australia, Saudi Arabia, Poland, Turkey, Qatar, and the Czech Republic. The LoI between Indonesia and the United States, for example, aims to provide a framework for encouraging cooperation and capacity building in cyberspace between the two countries. It has the scope of cooperation in several areas, including discussions on the development of national cyber strategies, national incident management capabilities, cybercrime capacity and cooperation, multi-stakeholder partnerships, promotion of cybersecurity awareness, and cooperation in other relevant regional places accordingly.

So far, in the execution of areas of cooperation that have been agreed upon in the Indonesia-US cyber cooperation, BSSN established communication through the US Embassy in Jakarta, and it was this embassy that bridged coordination and cooperation in the cyber field, for example with FBI representatives. Currently, the collaboration carried out is information sharing related to the threat of cyberattacks and increasing human resource capacity through webinars and training. From the BSSN side, one of the indicators referred to is the number of BSSN cyber human resources who have received capacity building under the RI-US cyber cooperation, and another related to anticipation or action steps to reduce the impact of the threat of cyberattacks as a result of information sharing cooperation between the two parties. One of the challenges that BSSN faces in executing cooperation agreements is administrative problems where there is often a discrepancy in the timing of program implementation between BSSN and the U.S. Embassy. In addition, just as the issue of cybersecurity is a cross-sectoral issue, coordination with other cyber-related agencies is also an obstacle that BSSN anticipates.

Thus, having a cyber cooperation relationship with a strong country, of course, will also strengthen and increase Indonesia's cyber capacity. This is also Indonesia's strategy to gain access to the latest cyber technology from the U.S. through experience and knowledge sharing as one of the areas of cooperation. So far, the most frequently implemented cooperation is the sharing of information related to vulnerabilities that exist in the cyber domain, both those that already exist in the cyber domain of the Republic of Indonesia and those that are happening in the global cyber domain.

Related to cyberterrorism, it is also the scope of cooperation, collaborating together with the National Counterterrorism Agency (BNPT). For information, Indonesia-US cooperation in the cyber sector can also be a reference for cross-cooperation between government agencies. The U.S. Embassy and BSSN has established a kind of information sharing mechanism related to existing and future cyber threats, then implemented capacity building programs, and strategic dialogues in the field of cybersecurity involving cybersecurity entities in each country. So far, in the execution of areas of cooperation that have been agreed upon in the RI-US cyber cooperation, BSSN established communication through the US Embassy in Jakarta, and it was this embassy that bridged coordination and cooperation in the cyber field, for example with FBI representatives.

a. Capacity Building

The entry of the digital continuum into all spheres of human activity makes it impossible to consider cybersecurity as a distinct policy area. On the other hand, cyberspace has become a cross-cutting policy issue. At the same time there is an awareness that no country or organization is 'cyber-ready'. Increasing the capacity of all stakeholders to fully benefit from digital technology and addressing the challenges that come with it has become a common thread. Therefore, capacity building is an overarching concept that applies to all the cyber fields mentioned above. This relates to efforts to 'create, develop and maintain institutions and organizations capable of learning and bringing about their ongoing transformation, so that they can play a more dynamic role to sustain the national development process'. (United Nations, 2002).

Training programs and courses to improve cybersecurity skills should be conducted in coordination with the Defense Cyber Operations Center. Training for human resources on the importance of cybersecurity needs to be held to increase understanding of preventive measures to prevent cybercrime. In order to develop the capabilities of human resources in dealing with cybersecurity, the TNI has collaborated with several stakeholders who are experts in the field of information technology. One of the stakeholders is Del Institute of Technology (IT Del), North Sumatra. The cooperation is planned to last for three years, from 2014 to 2017, with three programs namely the preparation of a cyber warfare model, a military cyber intelligence seminar and cyber operations, and a cyber camp or cyber weekend. (Rizal & Yani, 2016).

From the analysis that has been carried out, the author has ensured that capacity building is a very important element for every country because the capacity building program is always present in every cyber cooperation agreement between various countries, in a world where technological developments and the increasingly massive use of the internet result in activities in cyberspace are also getting more intense. Realizing this, each country will certainly do everything to increase the capacity of their respective SDM skills and of course to achieve this, cooperation with other countries or in particular countries that have better capacities is one of the most effective ways so it is not surprising that many countries do the same.

As previously explained, all cyber affairs easily become cross-border affairs which means cooperation with other countries is an inseparable aspect both within the scope of capacity building and others. As Citra Yuda Nur Fatihah, a diplomat of the Indonesian Ministry of Foreign Affairs, has said that the cyber issue is a very important issue and will continue to grow in significance as time passes, because this is the improvement of human resource capacity is very crucial, especially for developing countries that must pursue the capabilities of developed countries, especially with the absence of concrete international regulations that regulate how a country should act in the world cyber that makes violations of sovereignty can easily occur and of course developing countries are the most vulnerable to being affected.

The author concludes that there are important aspects contained in cross-border cooperation in the concept of capacity building, namely:

1. Engage with partners and international organizations to support the development of legal, organizational, and technical skills to counter cyber threats
2. Assisting various communities in making policies such as political, legal, technical in an effort to strengthen their capacities through training, development or adaptation of relevant national policies, strategies, and institutions.
3. Support the development of secure technologies and networks in partner countries, including by facilitating public-private partnerships for cybersecurity in emerging and underdeveloped markets.
4. Promote good practices that respect fundamental or basic rights such as the protection of intellectual property and personal data.

Because basically it is needed not only to ensure the development of all countries in this world in the capacity of handling the cyber world but also there must be harmonization in the cyber world which has so far been too anarchic because there are no binding regulations, so it takes awareness for various countries in the world to have a sufficient fundamental basis to respect each other and this can be realized with the many capacity building collaborations between one country and the others although of course there will be challenges because there are still countries that carry out cyber cooperation with political objectives such as with the formation of The Five Eyes which certainly has practitioners who can violate the sovereignty of other countries, not only that, even the establishment of the LoI between Indonesia and the United States which discusses cyberspace is also backgrounded by political elements where the concerns of the United States in the development of Chinese Technology and also in the Indo-pacific issue where the US hopes that with the holding of this cooperation, Indonesia can become a partner of the US in dealing with the issue that is considered a problem.

For example, there are activities that have been carried out by BSSN with America, namely the Virtual Homeland Security Investigation (HSI) Online Investigation which will be held on March 14-16, 2022. This activity was initiated by the U.S.Embassy and invited BSSN as one of the participants. The delegation from BSSN was personnel of the Directorate of Cybersecurity Strategy and Ciphers. The results of this activity are:

1. Develop the ability to investigate, address, and analyze digital evidence in an effort to combat transnational crime and human trafficking
2. Conducting discussions on transnational crimes, digital forensics, dark site investigations
3. Information exchange as well as best practices in efforts involving cyber networks.

It can be understood that in this activity there are two programs that are the main focus, namely capacity building and information sharing which are the two programs that the author values as the focus of increasing the capacity to deal with cyber threats.

b. Information Sharing

Not only assets, but many developed countries also cooperate to obtain this valuable information where for example is the formation of the Five Eyes where five developed countries that have high capabilities unite to capitalize on the cyber world. In addition to the cooperation that is business collaboration as mentioned, there is also a lot of cooperation carried out by developed countries with developing countries that have the urgency to improve the handling of cybersecurity and of course to do this assistance from more proficient countries will be a very interesting option such as cyberspace cooperation between Indonesia and America where Indonesia is intensively developing by expecting guidance from the US.

So what is the attraction for developed countries like the US to cooperate with countries that are arguably subordinate to them in a cyber context? Of course, returning to the aspect of information that is the main commodity in cyberspace, developed countries expect reciprocity of information exchange that is considered commensurate over the two countries. For example, the U.S. and Indonesia, the U.S. agreed to provide information related to human resource development, relevant regulations and policies, as well as a suitable and replicable institutional model or system, while to pay for the assistance, Indonesia must become a U.S. partner in political aspects related to sensitive information such as Indo-pacific issues and China's technological developments that are being continuously monitored by the US. The importance of information in cyberspace is supported by Welly Puji Ginanjar, a Data Processor at the Directorate of Cybersecurity Strategy and BSSN Password that between BSSN and the United States side, especially the FBI, continues to strive for the exchange of information between the two sides. Information Sharing is also ultimately the aspect of cooperation that is most often carried out by the two countries.

The importance of Information sharing actually goes back to the concept of Cyberpower, because as Kuehl (2009) said Cyberpower has always been a measure of the ability to use cyberspace. Technology is one of the obvious factors, because it is the ability to 'enter' the cyber world that makes it possible to use it. That technology is constantly changing, and some users such as countries, societies, non-state actors, etc. may be able to leapfrog the old technology to deploy and use the new ones for dramatic gains. By having a lot of information obtained through cyberspace, a country can increase the cyberpower factor they have and then by this can provide soft power when formulating policies with other countries and also in politics or in this case cyberpolitics in the international world which ultimately gives great benefits to the country. The concept of power itself has been widely understood that it can change the decisions of a country or worse it can create hegemony. Aspects of cyber threats that want to be faced by sharing the right information, of course, include the threat of cyber terrorism, an effective information sharing program can certainly help a country in dealing with the threat of cyber terrorism.

c. Handling Cyberterrorism

In handling Cyberterrorism in Indonesia, the two organizations, namely BSSN and BNPT, collaborate across sectors to enable effective handling. With the implementation of cyberspace cooperation between Indonesia and the United States, cybersecurity is one of the most important issues discussed in the cooperation and of course the issue of cyberterrorism is also one of the sectors that will be discussed. It is hoped that through this collaboration, Indonesia through BSSN and BNPT can develop in dealing with cyberterrorism because as it is known that the United States is a country that massively fights terrorism around the world and certainly has a growing handling of cyberterrorism.

Over a three-year period, Indonesia was one of the most heavily armed Asian countries. For example, in 2015 the number of terrorism crimes in Indonesia was 1,143 cases and in 2016 it increased to 1313 cases. The number of terrorism cases in Indonesia has increased more and more in 2017-2022 now. A number of these terrorism crimes have been detected and arrested through the internet network by the Police, BNPT, bloggers, YouTubers and other netizens. Increasing the escalation of acts of terrorism in Indonesia, the Indonesian government is required to move quickly to take action based on existing laws and regulations. So far, to ensnare parties who spread hoax news, hatred, hostility, do not accept differences and lead to radicalism will be entangled with Law No. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law). (Hatta et al., 2018)

The author believes that the seriousness of the two countries in facing the urgency of the threat of cyberterrorism can be seen from the existing cooperation. In addition to the LoI on cyberspace between Indonesia and the United States, Indonesia represented by the BNPT also has a cooperation with the United States, namely "Memorandum of Understanding between the Government of the Republic of Indonesia and the Government of the United States of America on Strengthening Counter-terrorism Cooperation." With these two collaborations, the handling of cyberterrorism in Indonesia handled by BSSN and BNPT will work closely with the United States and is expected to provide significant developments in capacity building in the face of the threat of cyberterrorism. In an effort to achieve this goal, the BNPT visited the Terrorism Screening Center (TSC), which is a special division in the FBI which has also collaborated with BSSN. The agency is responsible for the management and operation of databases to monitor and screen persons involved in terrorism networks. The TSC is a vital part of the U.S. counter-terrorism government's early warning and interdiction network. The TSC maintains a database containing sensitive national security and law enforcement information regarding the identities of persons known or reasonably suspected of being involved in terrorist activities to support frontline screening agencies in identifying terrorists suspected of attempting to obtain visas, entering the country, boarding planes, or engaging in other activities.

In modern times where technology and internet use are increasingly massive which causes the use of cyberspace to be more intense, so are terrorists who also realize the many opportunities that are present because that is why proper and consistent tracking is needed. The author realizes that this urgency is very relevant to the BNPT's visit to the Terrorism Screening Center (TSC) managed by the FBI, the TSC owned by the FBI is a resource that uses cutting-edge technology and of course that allows the FBI to dive into cyberspace and find potential threats. This kind of thing should be adopted by Indonesia, the existence of TSC in America is very helpful in handling cyberterrorism and it can be seen that BSSN who is responsible for cybersecurity should be able to cooperate with the FBI to obtain a transfer of technology and transfer of knowledge in order to allow Indonesia to create its own TSC.

After conducting an in-depth analysis, the author can formulate what are the types of cyberterrorism threats that Indonesia will often face in the future, namely:

1. Propaganda. The Internet is used by terrorists and their organizations to disseminate and manage their advertising through information warfare, to instill their ideology, to conduct psychological warfare and to radicalize and recruit new members from all over the world, through terrorist websites, online magazines, and various social media platforms
2. Communications and Networking. Terrorist groups have used social media platforms and encrypted messaging system applications (such as Whatsapp, line, youtube, twitter), online game chat rooms, coded messages or steganography for secret discussions, direct and private communication purposes (which include networking with other group members, interactions with new members and supporters), planning and coordinating physical attacks and planning hacking operations.
3. Fundraising. Financing of terrorist activities (acquiring weapons or supporting war efforts by providing funds to the families of fighters) is no longer carried out through charitable organizations alone but is also carried out with donations through social media platforms and blogs, and the use of digital currency bitcoins.

With this, the identification of threats should have been seen and can be handled with the collaboration of the two bodies, namely BSSN and BNPT. BSSN will be responsible for tracking and also analyzing threats through cyberspace and BNPT can take direct action or follow the direction of the findings identified by BSSN. This plan should already be on the agenda of the BSSN and BNPT as informed by Welly Putri Ginanjar that collaboration with the BNPT is continuing with the BNPT as the main actor. (Appendix to Interview with Welly Putri Ginanjar, 2022)

As Gabriela Luca (2017) has explained that Cyberterrorism can be understood as a convergence of terrorism and cyberspace. In this case, threats or attacks on computers in which the network and the information stored in it are aimed at intimidating the government and/or society for political or social purposes. To meet the classification of cyberterrorism, it is necessary to take action through cyberspace that can at least threaten a country. Here it can be understood that effective collaboration between BSSN and BNPT is needed to be able to deal with the threat of cyberterrorism.

Then how to make the collaboration effective? The author believes that the key lies in how BSSN can capitalize on the LoI of cyber cooperation with the United States that exists, namely specifically in aspects or programs of capacity building and information sharing, if BSSN can maximize cooperation in the two aspejs, the handling of cyberterrorism that will be executed by the BNPT is considered to have experienced significant developments because as a result of interviews that have been conducted by Citra Yuda Nur Fatihan that the increase in cyberterrorism that will be executed by the BNPT is considered to have experienced significant developments because as a result of interviews that have been conducted by Citra Yuda Nur Fatihan that an increase in the improvement of cyberterrorism that will be executed by the BNPT is considered to have experienced significant developments because as a result of interviews that have been conducted by Citra Yuda Nur Fatihan that the increase in

cyberterrorism that will be executed by the BNPT is considered to have a significant development because as a result of interviews that have been conducted by Citra Yuda Nur Fatihan that the increase in cyberterrorism that will be executed by the BNPT is considered to have a significant development because as a result of the interviews that have been Human resources entering the cyber world are the most important factor for the issues in this thesis. (Appendix to Interview with Citra Yuda Nur Fatihah, 2022)

Conclusion

After all the analysis that has been carried out, the author can draw the conclusion that the implementation of cyberspace cooperation between Indonesia and the United States to increase the capacity to handle cyberterrorism in Indonesia can be considered less than optimal. The opinion given by the author is also supported by the Directorate of Security and Cyber Strategy of BSSN where it is said that the significance of the implementation of the cooperation carried out is not as much as expected. The capacity building and information sharing program, which is considered as the most important aspect of this cooperation, has not been able to be carried out as observed because BSSN is still constrained by communication problems with the United States or especially the FBI. This communication problem arises because BSSN to communicate with the US side must first go through the embassy before it is finally conveyed to the relevant parties, this communication line is considered ineffective because it takes a long time to be realized which causes both capacity building and information sharing programs to be involved in obstacles and ultimately has an impact on the implementation of handling cyberterrorism threats. The author thinks that Indonesia and the US should have a fast and direct communication mechanism as is the case in cyber cooperation carried out by Japan and the US where communication is not an obstacle.

References

Ariesta, M. (2019). Keamanan Siber Jadi Perhatian Khusus Indonesia dan Australia. Keamanan Siber Jadi Perhatian Khusus Indonesia dan Australia - Medcom.id (Accesed 24 May 2022).

Billo, C. G., & Chang, W. (2004). Cyber Warfare an Analysis of the means and motivations of selected nation states. *Office*, *December*, 142. http://scholar.google.com/scholar?hl=en&q=CYBER+WARFARE++AN+ANALYSIS+OF+THE+MEANS+AND+MOTIVATIONS+OF++SELECTED+NATION+STATES+&btnG=&as_sdt=1,5&as_sdtp=#0%5Cnhttp://www.mendeley.com/research/cyber-warfare-analysis-means-motivations-selected-nation-states/.

Chen, T.M., (2013). *An assessment of the department of defense strategy for operating in cyberspace*. Army War College Carlisle Barracks Pa Strategic Studies Institute.

Choucri, N. (2013). Cyberpolitics in international relations. In *Choice Reviews Online* (Vol. 50, Issue 12). https://doi.org/10.5860/choice.50-6993.

Golose, Petrus Reinhard. (2015). Invasi Terrorisme Ke Cyberspace. Jakarta: YPKIK.

Hatta, M., Rajamanickam, R., Abdullah, D., Hartono, H., Saleh, A. A., Djanggih, H., Bunga, M., Wahab, M., Susena, K. C., Abbas, I., Aswari, A., & Sriadhi, S. (2018). Internet and Terrorism in Indonesia. *Journal of Physics: Conference Series*, *1114*(1). https://doi.org/10.1088/1742-6596/1114/1/012080.

https://www.dhs.gov/cybersecurity (Accessed 23 November 2021).

Juned, M., Bainus, A., Saripudin, M. H., & Pratama, N. (2022). *The dynamics of the USA and China*

*relations in the cyberspace: struggle for power in a global virtual world in building a global cyber regime Mansur Juned * Arry Bainus, Mohamad Hery Saripudin and Nugraha Pratama*. *30*, 396–414.

Juned, M. (2017). Mapping of Islamic Firqa Terrorism Movement in Indonesia. Malaysian Journal of Social Sciences and …, 2(3), 64–71. http://www.msocialsciences.com/index.php/mjssh/article/view/49.

Juned, M., Samhudi, G. R., & Akhli, R. A. (2022). The Social Impact of Expanding the Indonesian Military Mandate on Counter-terrorism Implikasi Sosial Perluasan Tugas Tentara Nasional Indonesia dalam Kontra Terorisme. 13(1), 105–115.

Kuehl, D. T. (2011). From cyberspace to cyberpower: Defining the problem. Cyberpower and National Security, 24–42.

Luca, Gabriela. (2017). "Manifestations of Contemporary Terrorism: Cyber-terrorism", Research and Science Today, pp. 20–25.

National Cyber Investigative Joint Task Force — FBI (Accessed 23 November 2021).

Nusantara, Abdul Hakim G. (2003). Undang-Undang Pemberantasan Tindak Pidana Terorisme Dalam Perspektif Negara Hukum. Bandung: Badan Pembinaan Hukum Nasional.

Kemmerer, R. A. (2003). Cybersecurity. *Department of Computer Science University of California Santa Barbara*, *6*, 1–23.

Obotivere, B. A., & Nwaezeigwe, A. O. (2020). Cyber Security Threats on the Internet and Possible Solutions. *Ijarcce*, *9*(9), 92–97. https://doi.org/10.17148/ijarcce.2020.9913.

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967.

Setiyawan, A. (2019). National Cybersecurity Policy in The U.S. and Indonesia. *Αγαη*, *8*(5), 55.

Todes, A. (2004). Grand international. In *Strad* (Vol. 115, Issue 1370).

United Nations. (2002). United Nations system support for capacity-building. *United Nations Economic and Social Council*, *2002*(58).

Valeriano, B. (2015). Cyber War Versus Cyber Realities: Cyber Conflict in the International System by Brandon Valeriano and Ryan C. Maness. Journal of Information Technology & Politics, 12(4), 399–401. https://doi.org/10.1080/19331681.2015.1101039.

Zainal A. Hasibuan, (2013). Indonesia National Cyber Security Strategy: Security and Sovereignty in Indonesia Cyberspace. Dewan Teknologi Informasi dan komunikasi Nasional

Copyrights