Terrorist Financing Through the Internet in Indonesia: Methods and Vulnerabilities

Ishna Indika Jusi[1], Aryana Satrya, Ph.D[2], Broto Wardoyo, Ph.D[3]
{ishna.jusi@gmail.com[1], aryanasatrya@yahoo.com.au[2], broto09@ui.ac.id[3]}

[1,2,3] Universitas Indonesia, Jakarta, Indonesia

Abstract. As a medium that facilitates various activities easily, safely, and has no geographical boundaries, internet is often misused by terrorists to support their activities. Terrorists continue to look for any chances to exploit various vulnerabilities on the internet system and network, in order to avoid the rules and pressure from the government. The existence of the internet indirectly expands terrorist activities, one of them is their funding. Through the internet, terrorists can raise funds with a wider, faster, anonymous, and greater amount. Thus, this paper aims to describe the terrorism funding method trends in the information and technology era in Indonesia, its vulnerabilities, and the recommendation to reduce the misuse of the internet by terrorists. To analyze this trend, the conceptual framework of the United Nations Office on Drugs and Crime (UNODC) is used which divides terrorism financing activities on the internet into four groups, namely direct solicitation, e-commerce, exploitation of online payment tools, and charitable organizations. This research was conducted using qualitative method, which the primary data was obtained through discussions with experts from Special Detachment 88 (Densus 88), Indonesian Financial Transaction Reports and Analysis Center (PPATK), digital forensic experts, as well as journal literature reviews and reports from PPATK and Financial Action Task Force (FATF).

Keywords: internet, terrorism financing, Indonesia, vulnerabilities

1 Overview

The internet is now a global network of interconnected communication and information systems. An internet user in the world can access any information on the World Wide Web, communicate, share documents, store information, and even engage in commercial transactions together with millions of other internet users around the world. Besides providing broad access, the internet also provides anonymity that can be exploited by terrorist groups to collect funds from the supporters and sympathizers globally [11] Based on the Indonesian Financial Transaction Reports and Analysis Center (PPATK) report from 2011 to 2014, the electronic payment system; new payment methods; and payment via the internet has the highest risk with the value of 6.60, besides carrying cash (6.51), legal business (6.40), jewelry and precious metal trading (6.20), vehicles (6.20), and foreign exchange (5.26). PPATK assesses that the risk value of 5 to 7 is still in a moderate level, but a special treatment is needed so that the risk does not have the potential to go higher.

ICSGS 2019, November 06-07, Jakarta, Indonesia

DOI 10.4108/eai.6-11-2019.2297282

Table 1. Moving Terrorist Financing Method Risks [18]

No.	Terrorist Financing Moving Methods	Risk Value
1.	Through electroning payments (debit, credit, and prefunded cards) Through online payments (internet dan mobile banking) Through new payment methods	6.60
2.	Through cash or similar instruments within and across national borders (cash smuggling)	6.51
3.	Through legal businesses	6.40
4.	Through jewelry and precious metal trading	6.20
5.	Through motor vehicles trading	6.20
6.	Through foreign exchange business activity	5.26

The risk of online payment system tends to be higher than other methods because of the use of fake identity to open, trade, lend, or transfer account, the difficulty of monitoring and controlling the transaction system, and New Payment Methods (NPM) that is still not widely known which led to the potential of its misuse. Not only that, the internet seems to provide a 'virtual bridge' that can cross the national borders, so it enables terrorists to get a wider scope with a greater profit potential [2].

The high potential, speed, and global reach is proven by the 'Swift Attack' against the Bangladesh Bank in 2016 in the form of a single cyber-attack on bank. The attack was the result of hacking using malware to steal USD 101 Million or around IDR 1.3 Trillion in just one day and involved several countries. The high nominal obtained in a relatively short period of time is certainly attractive to terrorists [28]. In Indonesia, a similar case had occurred in 2010 to 2012. Rizky Gunawan, a private sector employee with his teacher, Marwan, succeeded in hacking the illegal Fintech which were then used for military training in Poso, and carried out attacks on Kepunton Bethel Full Gospel Church of Indonesia (GBIS) at Solo in 2011. Within two years, Rizky managed to get around IDR 6 Billion [17]. In terms of quantity, the funds obtained are far higher than physical robberies or *fa'i*. Abu Roban, an Indonesian terror group specializing in bank and gold shops robberies, is said to have received IDR 500 million from state-owned bank robberies [26].

Basically, the internet facilitates the financing infrastructure and fund transfer both traditionally, such as internet banking and credit card to various alternatives, such as Fintech, PayPal, and crypto currency that are constantly being developed. These developments in internet-based payments are then exploited by terrorists to fund their activities and avoid the tracking of its funding by law enforcement. Some researchers believe that innovations in financing terrorism are opportunistic, which they take the advantage of the weak supervision structure of the financial system of the country, especially, in terms of internet-based funding method. This innovation is very dangerous because it has the potential to provide new trends for other militant groups to emulate. The emergence of new forms of funding technology presents more innovative fundraising and transfer opportunities, provides new options besides the traditional methods, and enables the terrorist groups to achieve the autonomy and financial sustainability they want [12]. Thus, this article seeks to explore the ways terrorists fund their organizations through the internet, at the stage of collecting and transferring the funds under Indonesian law and the vulnerabilities faced by the government and the financial service providers.

2 Conceptual Frameworks and Method

Like most organizations, terrorists need funds to meet their needs [22]. According to some experts, funds are seen as a 'source of life' and a driving force of a terrorist organization. Without funding, terrorists will not be able to carry out their operation, attack, or even exist as an organization [9]. Broadly speaking, terrorism funds are allocated for two main activities, namely operational and supporting activities [21]. For the operational activities, the funds are used to meet their basic needs, such as food, shelter, transportation, equipment, and materials for making bombs. While, the supporting activities are referred to a propaganda, recruitment, fundraising, and training [3].

The funding sources used by the terrorist groups vary, from legal sources to illegal, directly or indirectly, such as using intermediaries, and from local to global. However, funding for terrorism is not only limited to money. Those who encourage, plan, and get involved in the process of their action can be categorized as terrorism funding also. As explained in Law Number 9 of 2013, Article 7, funding of terrorism is not limited to money, but all assets or objects that are either movable or immovable, tangible or intangible, in any form including digital or electronic format.

The process of depositing and transferring funds collected by terrorists determines their ability to carry out the acts of terrorism. The process usually involves parties and transactions outside the terrorism network directly, especially if the transaction needs to go through the formal financial sector, the process of transferring funds will be beyond their control. Because terrorism financing activities are becoming increasingly visible in the formal financial sector and law enforcement agencies, terrorists must find an alternative method to sustain their activities, one of which is through the internet.

Based on the 2012 United Nation Office on Drugs and Crime (UNODC) report [27], the use of the internet in terms of financing by terrorists is divided into four categories, which are: 1) direct solicitation, the terrorists request funds directly through website, chat group, and social media; 2) e-commerce 3) exploitations of online payment tools and new payment methods, such as virtual currencies and hacking at FinTech, and 4) charitable organization, which is used as a front to promote the ideology of their organization or to provide for their material needs. The primary data related to terrorism financing through the internet were obtained from discussions with members of Special Detachment 88 (Densus 88), Indonesian Financial Transaction Reports and Analysis Center (PPATK), and digital forensic experts. Whereas, the secondary data was obtained through Financial Action Task Force (FATF) and PPATK reports, as well as literature studies in journals that discuss funding of terrorism.

3 Terrorist Financing Methods and Its Vulnerabilities

In 2012, UNODC classified terrorism funding on the internet into four methods, namely direct solicitations, new payment methods and e-commerce, exploitations of online payment tools, and charitable organization. In this section, each method along with the examples of cases that occur in Indonesia will be explained.

3.1. Direct Solicitations

Direct solicitation refers to the use of sites, chat rooms, emails, and others to solicit and collect donations directly from their supporters. Since the September 11 tragedy, terrorists have increasingly used this method in terms of funding their actions. The following examples illustrate the direct terror financing on the Internet [11]:

> *"They used the Izz al-Din al-Qassam Brigade, the military wing of Hamas, to post on their website that recruits suicide bombers and encourages supporters "to*

contribute... what they can do to help Jihad and all resistance until the Palestinian Muslim community is freed and the occupation is removed" [4]

Hizbullah, through their television station, 'Al-Manar' has a website that urges the contribution "for the sustainability of the Intifada", and attaches a list of accounts in Lebanon to collect funds; The Global Jihad Fund publishes a website that urges donations "to facilitate the growth of various Jihad movements around the world by supplying them with funds for arms purchases and training". The site also attaches the bank account in Pakistan and links to the websites that support the terrorist organizations, including the Taliban, Laskar e-Taliba, Hamas, and Hizbullah.

Aside from commercial sites, other media that are used quite often by terrorists to conduct campaigns and raise funds directly are social media. Through social media, terrorists can reach a greater number of audience through peer-to-peer communication, which is done through chats and forums, social networks like Facebook, Twitter and Instagram, mobile applications for personal communication, such as Whatsapp and Telegram, or safer communication networks like Surespot and VoIP [8]. In Indonesia, requests for donation and fund can be in the form of explicit statements, such as those made by Mujahideen of East Indonesia (MIT) on social media (Figure 1). However, urgent requests are usually done by asking for donations directly to their supporters as in the case of Rio Adiputra (Figure 2) [29].

Fig. 1. Mujahideen of East Indonesia's Crowd Funding Campaign on Twitter [33]

Although the MIT fundraising process was carried out directly, MIT still used an intermediary account, the Abu Ahmad Foundation (AAF), a fundraising foundation from Indonesia that collected money to buy food, weapons, clothing and other materials for jihadists, as well as to open a new Telegram channel (memri.org). Whereas in Rio Adiputra case, ordered by Iron, he requested funds directly from the 'brothers' in Bima to be given to the 'Umahat' or the terrorists wives left by their husband because their husbands were shot by the police, imprisoned, or escaped, or the 'ikhwan' which incorporated in the Santoso group. He then received funds of IDR 1.5 million from Hafid, Fadli, Lahmudin, to buy tickets to Poso, buy explosives in the form of fertilizers, and rent vehicles [30]. As shown in Figure 2 below, social media in the form of a messenger becomes an effective mediator to raise funds for terrorists, without making people outside their network suspect them. Not only that, messenger like Whatsapp has encryption which makes it difficult to be intercepted by the authorities.

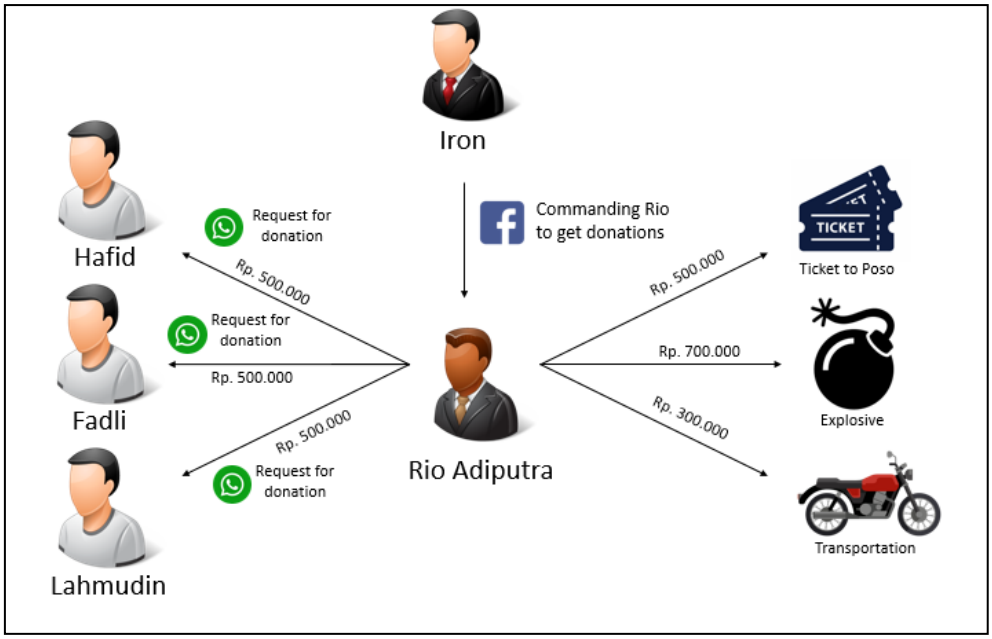

Fig. 2. Terrorist Financing through Whatsapp [18]

Although it is proven that there is abuse by the user, social media companies themselves are not included in terrorism funding. Generally, companies continue to work with the authorities to provide information, close, and block those accounts. In Indonesian law, social media is a form of Electronic System Organizer under the Regulation and supervision of the Ministry of Communication and Information. However, they do not have registration and licensing obligations to be able to operate in Indonesia.

Vulnerabilities. Social media is often misused by terrorists because of the easiness and quickness of creating accounts and accessing them, without requiring the use of IDs, e-mail addresses, and phone numbers as the user verification. Thus, a control is needed by the social media organizer which can be done in two ways, namely at the pre-account creation and post-account creation stages. The content control at pre-account creation stage is done through an agreement that is stated in the Terms and Conditions of the Service where all social media prohibits the existence of violence and terrorism content on their services, and will be penalized if violated. Meanwhile, the content control at post-account creation can be done with internal tools and the "report" feature on social media in the form of content-sharing, such as Twitter, Instagram, and Facebook. On the other hand, the content control by the government can be done through reporting and searching by Cyber Drone 9, the negative content search system owned by the Ministry of Communication and Information, which later, the content will be blocked, and the government can ask the social media provider to remove the content. However, in the case of social media in the form of messengers, such as Whatsapp and Telegram which have high-level confidentiality and security features, those forms of prevention are not effective. End-to-end encryption, secret message, and channel or broadcast message features make it difficult to track and eradicate terrorism content on social media [31].

The vulnerability to social media abuse is compounded by the fact that Indonesia does not have a data center for social media, so it needs to do mirroring to neighboring countries. This will certainly hinder the investigation process if there is any misuse done by the terrorists or

other crimes that have the potential to cause many victims (Ahmad Syafaat). Thus, Indonesia should have started to consider building an internet infrastructure in the form of an adequate server and data center. This is needed in response to the high level of public access to the internet today. According to the result of a survey conducted by Indonesian Internet Service Providers Association (APJII) in 2018, around 64.8% or 131.17 million of the total population of Indonesia, which is 264.16 million people have access to the internet.

3.2. E-Commerce

Sites that provide customer-to-customer buying and selling service are now very popular. The increase in e-commerce users is because the customers can easily access the sites anywhere, the sites are open to the public, the registration is very easy and fast, there is no face-to-face transaction, there is no procedure to verify and identify the customers, the customers can use anonymous email addresses, it has a fast transaction process, it enables users to register more than one user, and it facilitates various transactions across national borders. With all of these advantages, online trading sites or e-commerce are prone to be misused by criminals and terrorists [5].

In Indonesia, the case of terrorism involving the use of e-commerce is the Surabaya bombing happened on May 2018. Dita Oeprianto, along with his three children and his wife, blew themselves up in three different churches. The bomb he assembled was a TATP (*Triacetone Triperoxide*) type or often called the mother of satan by terrorists. According to the National Police Public Relations Head Setyo Wasisto, this type of bomb is a bomb that is easy to assemble, but has a high explosive power [16]. Based on the information obtained from PPATK, Densus 88, and the National Police Forensic Laboratory Center (*Puslabfor Polri*), several explosives were obtained through e-commerce Tokopedia gradually. The materials he got were fertilizer, acetone, ball bearings, lighters, and so on, which basically known as daily necessities but were vulnerable to misuse (dual-use goods). The easiness of getting these materials shows the lack of the monitoring processes and the awareness of the seller.

Vulnerabilities. With all the conveniences offered by e-commerce, such as fast registration, non-face-to-face transaction, the non-strict verification procedure, and so on, can actually backfire on the e-commerce itself. The terrorists or criminals can also easily carry out their transactions through e-commerce to transfer their funds. This was once carried out by an ISIS terrorist from the United States named Mohamed Elshinawy who received a fund of $ 8,700 or around 117 million rupiahs. To hide the origin of the funds, Elshinawy sells computer printers on e-commerce named eBay, then receives funds through PayPal payment that were allegedly sent by ISIS agents. Elshinawy said in the investigation process that he was ordered to use the funds for the operational needs of terrorism in the United States [25]. The following figure illustrates how ISIS agents send funds to Elshinawy via eBay.

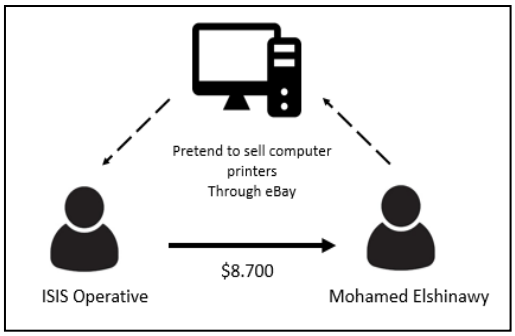

Fig. 3. Elshinawy's Terrorist Financing Ilustration [5]

Thus, to prevent the similar incidents, several approaches are needed to reduce and prevent the misuse by terrorism, such as: customer due diligence is needed by the service providers to the sellers, reporting on purchases of dual use goods with suspicious buying patterns, verification of information both sellers and buyers (such as address, e-mail address, IP address, identity of the credit card holder), implementing a system to detect any suspicious activity, reviewing abnormal activity, rejecting all transactions of prohibited items (weapons, drugs, etc.), postponing the transaction if an abuse is indicated, and maintaining the audit results data on all transactions and payments.

3.3. Exploitation of Online Payment Tools

The method of terrorism financing continues to develop in response to the technological advances and to avoid the fundraising process tracking and the law enforcement. The electronic payment methods, online, and New Payment Methods, which are now increasingly established, because a variety of vulnerabilities that continue to increase along with the increasing number of their uses. Many of these payment methods can be accessed globally to send funds quickly. Various online payment systems, such as PayPal to virtual currency, are also designed to maintain the user anonymity, which makes the system very attractive to be used as a tool for terrorism funding and money laundering, especially if the payment system is in jurisdiction with a weak AML/CTF regime [8]. Thus, this method and the online payment system have the highest vulnerability to be misused by terrorists.

Internet Based Payments. Internet-based payment method is part of the New Payment Methods (NPMs) that has developed in response to the market needs as an alternative to traditional payment. In some cases, this development has been driven by a demand for a safer and more convenient way to pay online. Whereas in other cases, the development of these payment systems is based on the desire to provide any access to financial services for those who are 'excluded' from the traditional financial services, such as individuals with poor credit records, minors, and residents from distant areas to access the bank. And finally, the development of online payment systems is assumed to have a positive effect on national and global economic development [6]. However, online payment systems as well as financial services and products in general, can be misused for the purpose of terrorism financing and money laundering.

One of the internet-based payment service providers that has been abused by terrorists is PayPal. PayPal is used to transfer funds of USD 1000 to Indonesia from Bahrun Naim who is located in Syria. The funds were sent to Munir Kartono, which then continued to Dwi Atmoko as the bomb maker, Nur Rohman as a suicide bomb martyr in Mapolresta Surakarta in 2016, and his wife for the living expenses and compensation for the death of her husband. Densus 88 mentioned that Munir Kartono, Nur Rohman, and Dwi Atmoko did not know each other. They only received orders directly from Bahrun Naim. When Dwi Atmoko handed the bomb to Nur Rohman, it was only marked by the code that Bahrun Naim had prepared beforehand. This makes it difficult for the authorities to track them. Not only that, from Figure 4 below it appears that the amount of money sent is insignificant, so it will not cause the redflag for the financial service providers.

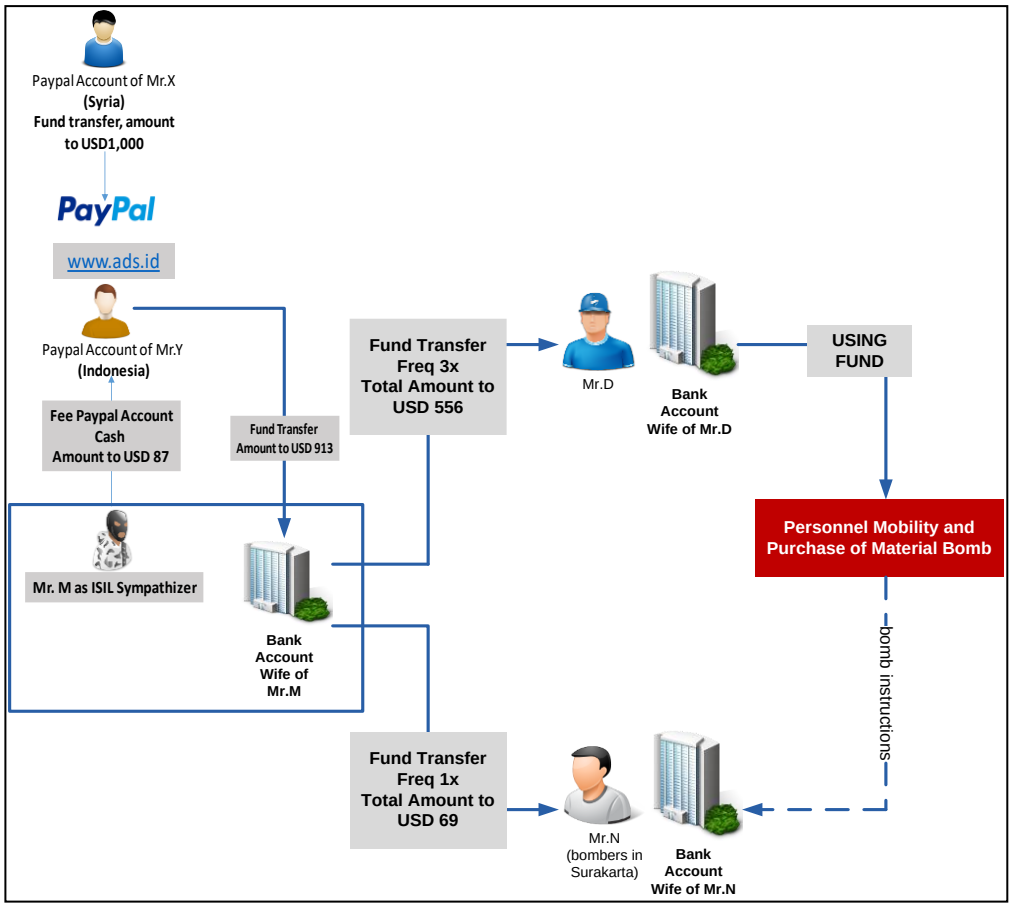

Fig. 4. Terrorist Financing Through PayPal [18]

Vulnerabilities. Basically, the term Internet Payment System is used to broadly describe the internet-based companies that provide online financial transaction services, such as PayPal to the consumers. In many cases, this internet payment system consists of non-bank financial institutions, making it possible for the service providers to not be subjected to the supervision and regulation and depending on the legal jurisdiction in which the system provides services to the consumers. The service has many advantages that are attractive to the consumers, but on the other hand, also becomes its own vulnerabilities, such as the non-face-to-face registration, the possibility of anonymous users, the limited human intervention, the fast transaction processing, across the countries, the high number of transactions, the limited competence of jurisdiction, and the difficulty of traditional financial institutions to monitor and detect any suspicious financial transactions [5].

Related to the vulnerabilities, FATF highlights the need for an online identity verification as the solution to help the internet payment service in reducing the risk of illegal activities. FATF considers that when the internet payment service monitors the transaction of its users adequately, especially related to the suspicious and deviate transaction patters from the profile

of the user, then the lack of face-to-face contact that occurs in the initial process of the transaction between the service provider companies and the users might not be a problem. Therefore, the service providers must continuously monitor and analyze the transactions, especially when it comes to sanctioned countries such as Syria, even in a small amount. Considering that the transactions are carried out internationally, cross-border cooperation becomes the key in countering terrorism financing and money laundering (ML/TF). In addition, the internet-based payment method such as PayPal is also vulnerable to hacking, as happened in the case of Krebs. In 2016, Krebs, a security analyst, claimed his PayPal account had been hacked. Funds in his account were almost taken and sent to ISIS in two trials. According to Krebs, PayPal does not have a modern authentication system, so it's easy to hack [1]. This kind of incident certainly could happen to any financial services through the internet.

Virtual Currency. Virtual currencies are digital objects that have economic value, and function the same as fiat currencies (government-issued). Virtual currency like Bitcoin, not only provides great opportunities in terms of financial innovation, but also has attracted the attention of various criminal groups and brought up a risk of terrorism financing and money laundering. This technology allows people to transfer their funds internationally and anonymously. If previously, currency purchases can be easily seen, identified, and traced through a formal banking system, all virtual currency transfers are very difficult to detect. According to the data obtained from the US Secret Service, criminals and terrorists are attracted to virtual currencies because they offer anonymity to the users until the transaction is carried out; have the ability to move illegal funds quickly from one country to another; have a lower colatility which led to a lower exchange rate risk; have been used by many criminals; and have high reliability [8]. Moreover, virtual currency has characteristics that give two advantages for terrorists, namely: 1) can be exchanged for fiat money and 2) high anonymity in its application.

In Indonesia, terrorism funding through virtual currency is used by Bahrun Naim network. According to Gunaratna [10], Bahrun Naim was a terrorist from Southeast Asia who first used the virtual currency Bitcoin. In December 2016, Bahrun Naim ordered Dian Yulia Novi to carry out a suicide bombing that was planned to be carried out at the State Palace as the main target, the Guards for DKI Jakarta Governor Basuki Tjahjapurnama, and the Brimob Mosque in Kelapa Dua. According to Densus 88 members, the funding of this project was sent by Bahrun Naim in Syria to Indonesia using Bitcoin. However, during the investigation, Dian admitted that she did not know the sender and the source of the incoming money and who the bomb maker is. She was only explained by her husband, Solikin that the funds were sent by Bahrun Naim (Densus 88) [32]. Until now, the Police and PPATK are still trying to trace the flow of funds from Bahrun Naim [24].

The innovation of financial technology such as virtual currency facilitates the cross-border payments, which in fact, makes no jurisdiction capables of strengthening the regulation of virtual currency transactions by itself. To overcome the misuse of virtual currency, a risk-based legal and regulatory framework is required as set by the FATF for the country. However, not all countries have a well-established legal framework to prevent the exploitation of virtual currency. This makes countries with weak laws become breeding grounds for terrorists and further worsens the global nature of terrorism. Therefore, the limited global scope of the AML/CTF regime becomes the primary challenge of the attempt. Setting the global standard will be very difficult because the financial and legal system growth in every country are different. In addition, the commitment between countries is also different, especially in combating terrorism. Not all countries are able to identify and assess current ML/TF risks, so they are also unable to mitigate the risks inflicted. Thus the global effort to overcome ML/TF

through virtual currency will only be as strong as the 'weakest link of the nation', due to the weak financial regulation and bad institution mechanisms [23].

According to Salami [23], there are at least two approaches that can be applied to investigate suspicious transactions using virtual currency. First, financial institution such as virtual currencies' exchanger must keep all the transaction records, including the information on parties involved, addresses, public keys, and number and date of transactions. Second, the investigation must focus on the exchanger to see any suspicious activity, considering the characteristic of the virtual currency that can be converted into fiat money. Through these two approaches, at least the process of tracking terrorism financing and other financial crimes can be done more easily.

3.4. Crimes towards Internet-Based Payment

Cybercrime is not a new thing. Basically, cybercrime is a traditional crime or physical crime committed online. Likewise, the crimes committed by terrorists on the Internet for their funding needs. In the early 2000s, terrorists often committed *fa'I* or physical robberies. Now terrorists are committing cyber robberies against FinTech. Terrorism organizations enter the cyberspace in terms of financing terrorism in order to avoid transactions in banks, which are closely monitored by the government and financial service providers, especially in the case of money laundering, and to reduce the risk of being caught while taking action. Through the internet, terrorists can also hide their identities when they do 'robbery' by hacking.

In accordance with the will left by Imam Samudera in 2004 before the execution, his successor jihadists are encouraged to study and practice hacking in committing terror. Over the past 10 years, the message has not been paid much attention. However, from 2010 to August 2012 Marwan and Rizki Gunawan, his trainee, managed to obtain around IDR 6 billion from the result of illegal FinTech hacking called speedline.com. Around IDR 500 million were then used for training in Poso and for the bombing in GBIS (Bethel Full Gospel Church) Kepunton Solo in 2011. Other than that, the funds obtained were also used to purchase assets for savings and will be used later when funds were needed for terrorist acts [17]. To prevent the similar cases from happening, a strict regulation is needed, especially regarding the illegal FinTech. Since the case occurred until 2019, there have been no specific legal regulations governing the illegal FinTech.

Vulnerabilities. As explained earlier, the internet becomes a significant source of instrumental power for terrorist groups. With the help of the internet, the ability of terrorist groups in terms of fundraising has increased. However unfortunately, the strategy made by the government to combat funding for terrorism is not always innovative, it is often hampered by bureaucracy, and the policies adopted are out of date (Napoleoni, 2016). This phenomenon is proven when terrorists have begun to use illegal FinTech that is not registered in the government to collect funds as has been done by Rizky Gunawan since 2010 through hacking. Until now, there is no law that regulates the problem. In fact, the government started to block the illegal FinTech at the end of 2018. This shows that the government is not responsive to the new threats due to technological and information development.

According to Laksmi [13], a strong regulation related to the strong internet-based payment services need to be established in Indonesia. This regulation must cover the risks related to the open internet system network, especially the non-face-to-face customer relations and anonymous digital transactions. Not only that, the policy must also measure the mechanism of the customer identification and verification process, and include a control and reporting system to be useful to identify suspicious transactions and report them to the Financial Intelligence Unit. Secondly, Laksmi considers that Indonesia needs to formulate a policy to overcome the problems and risks arising from the payments that are anonymous and have no geographical restrictions. These characteristics are considered to have increased the risk of identity fraud and the potential to facilitate illegal activities. In addition, to prevent hacking, the government must

ensure a strict enforcement of counter measures by the service providers to protect customer information [13].

Third, a comprehensive mitigation strategy is needed to reduce the risk of broad service segmentation. This strategy can include a guidance on the usage threshold mechanisms. Such a strategy can be implemented by issuing a guideline and requirement for the internet-based payment service providers and developing the centralized services to enable companies to monitor cross border transactions and assist the monitoring and evaluation process of the regulator. And finally, a strong cooperation is needed between the law enforcement agencies, regulators, and service provider industries through a coordination meeting, providing input to stakeholders related to innovations in financial technology and the security challenges. This kind of collaboration will certainly strengthen the existing law enforcement efforts in preventing and combating crime and terrorism activities in this sector [13].

3.5. Charitable Organization

Terrorist organizations often exploit charities as the intermediaries to raise funds in disguise. This method is very popular, especially among Islamic terrorist groups because they feel they have an obligation as Muslims to donate charity and zakat regularly. Tasnima Salsabila, a Hong Kong migrant worker who was affiliated with Bahrun Naim network, used her personal money to "donate charity" in the way of Allah because she believed that everyone who used part of their wealth to help the warring Mujahideen would receive the same rewards as the mujahidin who carried out *amaliyah* [20]. Thus, charity becomes a fertile field for the terrorists to exploit because people think funding the terrorist acts is part of their worship. In some cases, terrorist organizations even set up a charity with humanitarian purposes, such as helping victims of disaster, illness, poverty, etc., despite the fact that their funds can be used to fund the acts of terrorism or help the terrorist families. This was done to avoid blocking by the authorities. They collect the funds by asking for donations online to get a wide reach both locally and globally [8].

In Indonesia, Azzam Dakwah Center (ADC) was a charity based on social institution, charities, and da'wah formed by Jamaah Ansharut Daulah (JAD) and used as a front for the supporters of the Daulah Islamiyah. The da'wah center was run under the leadership of Azzam who was affiliated with ISIS. The funds were collected through the infusions of six *Qoriyah* (regions), namely Karanganyar, Klaten, North Solo, East Solo, Sukoharjo and Solo Raya. ADC was also often used to prepare for several acts of terrorism, such as making Molotov cocktails and canned bombs. The bomb was made by Suyanto to attack the Alfamart Surakarta shophouse conducted by Wahyudi, Candi Resto by Wawan Prasetiawan, and the private house of Candi Resto by Suyanto in November 2016. The three attacks were carried out based on the instruction from Nor Solikin, inspired by the chaos that occurred in Jakarta during Aksi Bela Islam, and a retaliation for the action of tearing the Quran that was allegedly committed by the owner of the Candi Resto restaurant [20].

Vulnerabilities. Terrorists will always cover their activities in various ways, one of which is by using a charity. "A fraud" planned by the terrorists to abuse charities is very difficult to track because of the guise of humanity and religion [8]. In Law Number 9 of 2013 related to terrorism funding, the criminal act of financing terrorism includes the funds that are intended for the terrorism activities, terrorist organizations, or terrorists. This regulation gives the terrorist a chance to send funds to the *ummahat* (wives of combatants) and terrorist families for their needs. Although the assistance is for humanitarian purposes, sending funds to the terrorist families has a high chance and risk that at any time, the funds can be used for the acts of terrorism. Therefore, it is necessary to review the regulation regarding the financing of terrorism, related to their wives and families considering the high risk of abuse.

In addition, a charity has a high operational capacity. According to FATF, charities have an access to large sources of funds from various parties, moreover the majority of funds obtained are in cash. Charities also usually have logistical networks that are broad enough to gather and send resources to support their operational activities. However, the wide coverage and network

they have create its own vulnerability. With a large number of members, a wide range of activities, and a large geographical distance, it is certainly difficult to implement an adequate control over the resources owned. When a charity has a humanitarian goal, their logistics network often flows into the areas of conflict with a low governance. These aspects increase the risk of abuse in the delivery of resources. To ensure that charities are not misused for terrorism activities, a good governance and strong financial management, internal controls and adequate risk management procedures are needed. Charities must also implement due diligence processes for individuals and organizations that send and receive the donation or cooperate with them, depending on the conditions and environment in which the charity operates [7].

To reduce the misuse of charitable and humanitarian foundations or organizations, it is necessary to conduct an audit by the authorities as well as transparency regarding the structures, beneficiary owners, place the charities into high-risk institutions, and make detailed financial reports. In addition, because charities rely on public trust, public awareness and caution as donors are also need to be increased in order to limit the flow of funds into terrorist institutions under the guise of humanity. The increasing number of online-based charitable institutions, such as Aksi Cepat Tanggap, Kita Bisa, and so on, which can raise funds quickly and reach the wider community, the government needs to educate the public through campaigns in proactive media in order to increase the awareness and caution about the danger of terrorism financing and money laundering through charitable institutions.

4 Conclusion

Criminals and terrorists have shown their adaptability and opportunistic nature in finding a chance to launder illegal money and fund the acts of terrorism. It is undeniable that the information technology development, such as the internet are increasingly expanding the access, opportunities, and reach of terrorist activities, including funding. Moreover, the internet is very easy to access, secure, has no geographical boundaries, can be anonymous, decentralized, and in some aspects, the regulation regarding this case is still weak. When the internet has become a global phenomenon, where everyone is easy to access, and commercial websites and payment systems via the internet have become more advanced, the potential and risk of abuse by criminal and terrorist organizations is also increasing. Terrorists are no longer dependent on the conventional method of funding, such as cash couriers, robberies, and through formal financial institutions. They take advantage of the development of technology and the internet, which they are able to collect large, fast, and anonymous funds through social media, e-commerce, internet-based payment services, and charities. All these conveniences, on the one hand, actually become the vulnerabilities and weaknesses to the system and application on the Internet.

References

[1] Krebs B. 2016 Reality: Lazy Authentication Still the Norm [Online]. USA: Krebsonsecurity.com; 2015 December 25 [updated 2016 December 15; cited 2019 August 15]. Available from:

[2] https://krebsonsecurity.com/2015/12/2016-reality-lazy-authentication-still-the-norm/

[3] Carrol P., Windle J. Cyber as an Enabler of Terrorism Financing, Now and in the Future. Journal of Policing, Intelligence and Counter Terrorism. 2018. 13(3):285-300.

[4] Clunan AL. The Fight Against Terrorist Financing. Political Science Quarterly. 2007. 121(4):569-596.

[5] Ezzeden Alqassam Brigades. Fundings [Online] 2004 [Cited in 2019 October 1]. Available from: http://fund.alqassam.ps/lang/en

[6] Financial Action Task Force. Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment System [Online]. 2008 June [Cited in 2019 September 5]. Available from:
[7] https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf
[8] Financial Action Task Force. Money Laundering Using New Payment Methods [Online]. 2010 October [Cited in 2019 September 5]. Available from:
[9] https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf
[10] Financial Action Task Force. Risk of Terrorist Abuse in Non-Profit Organisation [Online]. 2014 June [Cited in 2019 September 6]. Available from:
[11] http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf
[12] Financial Action Task Force. Emerging Terrorist Financing Risk [Online]. 2015 October [Cited in 2019 September 5]. Available from:
[13] https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf
[14] Freeman M. The Sources of Terrorist Financing: Theory and Typology. Studies in Conflict & Terrorism. 2011. 34(6):461-475
[15] Gunaratna R. Death of Bahrun Naim: Mastermind of Terror in Southeast Asia [Online]. 2018 [Cited 2019 October 2]. Available from: https://www.rsis.edu.sg/wp-content/uploads/2018/10/CO18161.pdf
[16] Hinnen TM. The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet. The Columbia Science of Technology Law Review. 2004. 5(1):1-42
[17] Keatinge T., Danner K. Assessing Innovation in Terrorist Financing. Studies in Conflict & Terrorism. 2019.
[18] Laksmi, SW. Terrorism Financing and the Risk of Internet-Based Payment Service in Indonesia. Counter Terrorist Trends and Analysis. 2017. 9(2):21-24
[19] MEMERI Jihad and Terrorism Threat Monitor. Indonesian Fundraising Group Abu Ahmed Foundation Continues to Encourage Supporters to Donate Using Cryptocurrencies [Online].; 2018 [Cited 2018 November 28]. Available from: http://cjlab.memri.org/latest-reports/indonesian-fundraising-group-abu-ahmed-foundation-continues-to-encourage-supporters-to-donate-using-cryptocurrencies/
[20] Napoleoni L. Terorist Financing. The RUSI Journal. 2006. 151(1):60-65
[21] Nathaniel F. The Mother of Satan: Bom yang Digemari ISIS & Mengguncang Surabaya. Tirto.id [Online] 2018 May 15 [Cited 2019 September 22]. Available from: https://tirto.id/the-mother-of-satan-bom-yang-digemari-isis-mengguncang-surabaya-cKqH
[22] Purwawidada F. Jaringan Baru Teroris Solo. Jakarta: PT. Gramedia; 2014.
[23] Pusat Pelaporan dan Analisis Transaksi Keuangan. Penilaian Resiko Indonesia terhadap Tindak Pidana Pendanaan Terorisme [Online] 2015. [Cited 2019 October 1] Available from:
[24] http://www.ppatk.go.id/backend/assets/images/publikasi/1499326479_.pdf
[25] Putusan Pengadilan Negeri Jakarta Timur Nomor 479/Pid.Sus/2017/PN Tahun 2017 (Ika Puspita Sari), Mahkamah Agung Republik Indonesia [statute on the internet]. 2017 [Cited 2019 October 2]. Available from: https://putusan.mahkamahagung.go.id/putusan/3dbe69ad674b4ba4ab33fb27d25a1e73
[26] Putusan Pengadilan Tinggi Jakarta Nomor 189/PID.SUS/2018/PT.DKI Tahun 2018 (Triyono), Mahkamah Agung Republik Indonesia [statute on the internet]. 2018 [Cited 2019 October 2]. Available from: https://putusan.mahkamahagung.go.id/putusan/a122d26dca902146eca8e97c26efe7df
[27] Realuyo CB. Following the Terrorist Money Trail. Connections. 2011. 10(2):105-124
[28] Reda HA. Terrorist Financing: Are Current Anti-Money Laundering Regulations Easily Applied to Virtual Currencies?. Colorado Technical University. 2017.
[29] Salami I. Terrorism Financing with Virtual Currency: Can Regulatory Technology Solutions Combat This?. Studies in Conflict & Terrorism. 2018. 41(12):968-989

[30] Sohuturon M. (2017) Polri Gandeng BI Usut Dana Bahrun Naim Lewat Fintech. CNN Indonesia [Online]. 2017 January 10 [Cited 2019 September 15]. Available from:
[31] https://www.cnnindonesia.com/nasional/20170110163454-12-185344/polri-gandeng-bi-usut-dana-bahrun-naim-lewat-fintech
[32] Stewart C., Maremont M. American Pleads Guilty to Accepting Islamic State Money to Fund Terrorism. The Wall Street Journal [Online]. 2017 August 15 [Cited 2019 October 3]. Available from:
[33] https://www.wsj.com/articles/man-accused-of-using-ebay-for-terrorist-funding-agrees-to-plead-guilty-1502811513
[34] Suhendi A. Ini Dia Sepuluh Lokasi Perampokan teroris Abu Roban. Tribunnews [Online]. 2013 May 14 [Cited 2019 September 17]. Available from: https://www.tribunnews.com/nasional/2013/05/14/ini-dia-sepuluh-lokasi-perampokan-teroris-abu-roban
[35] United Nations Office on Drugs and Crime. Use of Internet for Terrorist Purposes [Online]. 2012 [Cited 2019 October 1]. Available from:
[36] https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
[37] Zetter K. That Insane, $81 M Bangladesh Bank Heist? Here's What We Know. Wired [Online]. 2018 May 17 [Cited 2019 August 20]. Available from: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
[38] Conway M. Terrorist 'Use' of the Internet and Fighting Back. In: Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities Conference; 2005 September 8-10; Oxford, United Kingdom. Oxford: Oxford Internet Institute; c2005. p. 1-34.
[39] Putusan Pengadilan Negeri Jakarta Timur No. 776/Pid.Sus/2015/PN Tahun 2015 (Rio Adiputra alias Rio alias Abu Ridho alias Wewe Bin Yamin). Mahkamah Agung Republik Indonesia [statute on the internet]. 2015 [Cited 2019 September 29]. Available from:
[40] https://putusan3.mahkamahagung.go.id/search.html?q=denie&page=39
[41] Irawan P., Mardiansyah. Terrorist financing methods and vulnerabilities in New Payment Methods [interview]. Interviewer: Jusi I. 2019 Oct 1 [cited 2019 October 2].
[42] Indra M. Bahrun Naim's funding methods [interview]. Interviewer: Jusi I. 2019 Sept 16 [cited 2019 September 17].
[43] johny2b. Beware & be vigilant of efforts to gain supporters, win hearts & collect funds. Courtesy of @TRACterrorism. @DivHUmas_Polri @BNPTRI @BIN_Official: https://twitter.com/johny2b/status/1056099912796930053?s=09 2018 Oct 27 [cited 2019 September 23] [Tweet]. Available from: @johny2b.