



Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
January - June 2021. Vol. 15(1): 50–64. DOI: 10.5281/zenodo.4766532
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

This is a Diamond Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.



A Rational Choice Analysis of ISIS Mujahid in Becoming Cyber-Jihadists

Petrus Reinhard Golose¹

ORCID ID: 0000-0002-9952-7421

Abstract

One of the evils of globalization is the increased use of communication and information technology and social media to spread radical ideologies. In Indonesia, such cyber-jihad groups have emerged that replicate the Islamic State in Iraq and Syria (ISIS), and openly spread radicalism through the media. The objective of this qualitative study was to examine the phenomena that lead to becoming cyber-jihadists. Data were collected using in-depth interviews from five sources including AVR, WA, AH, MS, and RW. The participants of the study comprised prisoners of terrorism arrested for propaganda, funds collection for online terror activities, and disseminating information related to ISIS and radicalism in Indonesia. A rational framework based on rational choice theory (RCT) was adopted to understand the cyber-jihadist phenomenon, premising that cyber terrorism could become rational despite being considered as irrational. It analyzed the perpetrators' rationality to decide in becoming a cyber-jihadist using rational choice theory. The results are in line with the study of Cornish and Clarke (1986) that 7 rational choice structures were considered by the participants including: availability, method awareness, expertise needed, resources required, time required to commit, risk of apprehension, and moral evaluation. The study will be a useful contribution to the domain of literature as it will provide useful insights to administrators, police officials and the policy makers to combat jihad and prevent the use of social media in spreading terrorism.

Keywords: terrorism, cyber-terrorism, rational choice theory, social media, jihad

Introduction

Indonesia is one of the countries in Southeast Asia that experienced the most threats and attacks by terrorism (Junaid, 2013). Initially, terrorists focused attacks on western symbols such as foreign citizens and embassies but later shifted it to the police, places of worship, and other public spaces (Sanur, 2018). In Indonesia, there are continuous terrorist activities because its existence is a serious threat to state's integrity and sovereignty (Kurniawan & Primawardani, 2019). Kurniawan and Primawardani (2019) cite that terrorism leads to violence and insecurity at the national and international levels because it has a wide network. Ansori (2019) assert that this phenomenon is essentially a method of attack and not a philosophy or even a movement because it maximizes media exposure to affect the existence

¹ Indonesian Police College, golosepetrus88@gmail.com, ORCID ID: 0000-0002-9952-7421

of terrorists (Campos & Gassebner, 2009). The media spreads the radicalism invasion through the internet because the world no longer requires a physical presence. Above all, cyberspace has triggered the birth of the "lone wolf" where terrorists work alone without a herd. According to Iskandar (2020), they have an understanding of being radical without minding the physical presence of their indoctrinated people.

Undoubtedly, the era of globalization has caused an increase in the use of the communication media by the terrorists, who adapt their abilities to the available communication and information technology (Sarinastiti & Vardhani, 2018). Iskandar (2020) exposes radical ideologies using social media and the internet spreading and recruiting more followers. Radicalism is a stage or a step towards terrorism, since terrorists and suicide bombings who commit destructive actions are radically biased and fundamentally inclined to religious matters (Sari, 2017). They seem to replicate the Islamic State in Iraq and Syria (ISIS), that openly spread radicalism through the media (Shehata, 2015). According to the Indonesian National Counterterrorism Agency (BNPT), ISIS's main field is in cyberspace. Sari (2017) showed that this terror group allocates 50% of its finances for media activities. This enabled Abu Bakr Al-Baghdadi (the ISIS leader) to wage a jihad war. The Jihad was mainly carried out using destructive or violent attacks via telegram (CNN Indonesia, 2018). Furthermore, ISIS built media and public relations capacity using slogans such as "Enduring and Expanding" as well as displaying various videos of its military victories through the internet (Emina & Ikegbu, 2020; Haykel, 2016; Karjo & Ng, 2020).

BNPT took a decisive step by blocking several accounts on social media containing radicalism and terrorism content (Iskandar, 2020). This is in line with BNPT's policy not to encourage such terrorist groups that use Blogs, Facebook, Twitter, BlackBerry Messenger (BBM), WhatsApp, Line, and Telegram (Badan Nasional Penanggulangan Terorisme (BNPT), 2016; Sari, 2017). Suring 2009 to 2019, 11,803 internet accounts were blocked containing radicalism and terrorism content. According to the Directorate of Information Application Control, Directorate General of Informatics Applications, and Ministry of Communications and Informatics, 8,131 online messages were blocked on Facebook, Instagram, and Twitter. Meanwhile, 678, 614, 502, and 494 contents were blocked on Google/YouTube, Telegram, Filesharing, and websites respectively (Joffroy, 2020; Kominfo.go.id, 2019). The Ministry of Communication and Informatics continues to search several websites or platforms using the AIS engine every two hours despite the closure of radicalism, terrorism, and separatism online messages (Kominfo.go.id, 2019; Suard, 2020). Basit (2020) observed that Covid-19 served as a great opportunity for terrorists to spread radicalism. Simons and Cristina (2020) also showed that the practice of social distancing during this pandemic caused significant vulnerabilities in the community. Furthermore, the way people stayed at home enabled them to be free and be carried away on the path of radicalization by extremist and terrorist groups through the internet (Simons & Cristina, 2020).

Method

This study is qualitative in nature because it aims to obtain the phenomena that occur with cyber-jihadists. Data were collected using in-depth interviews from five sources including AVR, WA, AH, MS, and RW. The participants of the study comprised prisoners of terrorism arrested for propaganda, funds collection for online terror activities, and disseminating information related to ISIS and radicalism in Indonesia. A detailed demographic information about the five sources is presented in Table 1:

Table 1. List of Participants (interviewees)

Interviewees	Group Related	Age	Education	Job	Income (Per Month)	Arrested
AVR	<ul style="list-style-type: none"> • AT Tauhid • KD part 2 • M Admin Pembela Tauhid Group 	28	High School (Graduated)	the employee in a cellphone stall	IDR 750.000 (around \$52.8)	1st Oct 2018
	<ul style="list-style-type: none"> • Al Kahfi • Muhajirin At Tauhid (MAT) 	26	University (Graduated)	street food seller	around IDR 750.000 - IDR 1.500.000 (around \$52.8 - \$105.4)	8th June 2020
AH	<ul style="list-style-type: none"> • Al Kahfi • Muhajirin At Tauhid (MAT) 	28	University (Not Graduated)	convection employee in a home industry	IDR 1.500.000 (around \$105.4)	8th June 2020
	<ul style="list-style-type: none"> • Al Kahfi • Muhajirin At Tauhid (MAT) 	47	University (Not Graduated)	distribution driver in an automotive dealer	IDR 2.500.000 (around \$175.9)	8th June 2020
RW	<ul style="list-style-type: none"> • Al Kahfi • Muhajirin At Tauhid (MAT) 	31	University (present)	College Student	-	18th June 2020

Rational Choice and Terrorism

This study adopted the Rational Choice Theory (RCT) as an analytical tool to examine terrorism as an action of rational irrationality. In simple terms, the rational choice method enables the participants to maximize their utility in a research on terrorism. Nemeth (2017) defines this utility as a behavior to respect oneself, that includes the satisfaction that comes with the fulfillment of personal goals. Furthermore, such a utility proves to be a supportive altruistic action in helping friends, family, and strangers. Nemeth (2017) explains that the participants are required to meet three basic requirements to achieve maximum utility. First, an individual need to have a complete reference for a set of potential outcomes. Second, people believe that the result of "a" is better than "c" because "a" is higher than "b" that is superior to "c". Third, an individual accepts that the second requirement allows them to make a preference and rank the results from the best to the worst, as well as the ability to choose the most preferred outcome. Therefore, the rational choice method enables generalizing the human behavior, and predict as well as analyze the behavioral activities in econometric terms (Nemeth, 2017). Additionally, Nemeth (2017) points out that terrorists are rational actors that maximize their utility while operating under three basic assumptions. First, this terror group is motivated by stable and consistent political goals; second, terrorism is an action that is decided while other forms of political participation are closed; and third, terrorism is more effective than any other means.

A similar study by Akers (1990) had posited that: "Human actions are based on rational decisions and this means they are informed by the possible consequences of those actions... The rational choice theory explained that a person takes a criminal or legal action by maximizing outcomes and minimizing costs" (p. 654). According to Akers, a person's choice of being a rascal depends on a rational decision where there are considerations regarding the results and costs of the action. Nalbandov (2013) opined in similar fashion and showed that it is easy to detect terrorist true motivators and deal with terrorism if their behavior is more rational and predictable. Furthermore, Nalbandov (2013) explained that

there are several attempts to divide terrorism into a rational framework. This was in consistent with another study (Caplan, 2006), which looked at the specific rationality of terrorists.

Crenshaw (1981) attempted to divide terrorism into a rational framework by exploring the causes of this rascal action. This was later indicated in studies like Kydd and Walter (2006) and Pape (2003), that linked rationality with terrorists' strategic activities. Oberschall (2006) focused on the theory of collective action to describe terrorism into a rational framework. In addition, Libicki (2007) also examined the rational thinking behind terrorist motivations while van Um (2015) found that RCT used methodological individualism to explain collective behavior. Therefore, terrorist groups are regarded as unified actors reflecting a stable configuration of preferences and consistent goals (van Um, 2015). Furthermore, RCT allows to discover individuals as active and rational agents that determine the best course of action with certain rewards and costs. Shughart (2011) believes that terrorists calculate risk and make choices to get the greatest return in terms of “money, ammunition, and labor”. Korbl (2017) opines that terror groups change the tactics of such countries that impose countermeasures against them.

Cornish and Clarke (1986) have introduced the existence of a rational choice structure that is generally made by individuals while analyzing the rationalization of the perpetrators of crimes and their offenses. Table 2 exemplified a model rational choice structure:

Table 2 Model rational choice structure

Objective	Requirement
Availability	Number of targets Accessibility Methods of awareness
Resources	Cash yield per crime. Expertise needed Planning necessary Resources (e.g. Instrument of violence) Solo versus group assistance Time required to commit. Cool nerves
Risk factors	Risk of apprehension Severity of punishment (if caught) Confrontation with the victim. Identifiable victim. Social cachet (in the criminal world) Safe breaking versus mugging. Fencing (getting rid of any goods stolen, together with the main target, money). Moral evaluation.

Source: Cornish and Clarke (1986)

According to Cornish and Clarke, there are comprehensive rational decisions for every criminal in carrying out their actions. Therefore, this study adopted choice structures to identify and analyze the rational choices made by cyber-jihadists.

Cyber-Jihadist Phenomenon

Cyber-jihad is in line with the history of terrorism in the world because it originated from cyber-terrorism which is referred to as terrorist activities in and through cyberspace. Laytous (2021) has defined cyber-terrorism as “unlawful threats of attacks on computers, networks and the information stored while intimidating the government or its people”, preventing them to achieve political or social goals. These invasions cause fear, harm, and violence against people as well as property (p.2). Meanwhile, cyber-jihad uses technological tools and the internet to promote the idea of violent 'jihad' against 'enemies of Islam' (Hoffman & Schweitzer, 2015).

In various studies and existing facts, cyber-jihad is not concerned about supporting or complementary tactics such as propaganda, recruitment, communication, fundraising, attack preparation, and others to carry out Jihad war. Instead, terrorist tactics include digital vulnerabilities to invade and create terror, spy on law enforcement, or infiltrate specific organizations. For instance, the 9/11 attacks by the Al-Qaeda group was accomplished by taking control of aircraft through hacking of flight electronically and later hijacking it (Laytous, 2021). The presence of the Al-Qaeda group led by Osama Bin Laden was considered as a revival of terrorism and this led to the continuous practice of cyber-jihad in the world. This group also intended to globalize jihad internationally against the Jews and crusaders as well as to establish a caliphate.

The cyber-jihadists exploit the internet through several free and widely available technologies to achieve their goals. In addition, this group easily applies tactics that are very difficult for the authorities to restrict, a few of which are presented in Table 3:

Table 3 Internet tactics that cyber-jihadists exploit

Tactics	Method
<i>Encrypted Messages & Files</i>	It utilizes encryption technology to communicate online via email
<i>Codes & Steganography</i>	It uses an online coding method or program known as steganography where prohibited computer users hide information within messages, figures, or other files posted on the internet;
<i>E-groups</i>	It is a service offered by ISPs for users with similar interests to exchange messages;
<i>E-mail Dead Drops</i>	It involves distributing usernames and passwords for e-mail accounts to fellow terrorist cell members, whose information is stored in drafts. Therefore, no message delivery history will be detected
<i>Secure Web Sites</i>	It allows terrorist agents to exploit electronic mail services to communicate with members of their network;
<i>Hydra Web Links</i>	are used where multiple links to the same video or message are posted on a particular site or email chat room; and
<i>Spam Mimicking</i>	It utilizes the Spam Mimic Web site including http://www.spammimic.com and embeds encrypted messages in timescales to disguise the confidential data that was exchanged.

Source: (Davis, 2006)

Cyber-jihad continues to grow with the use of social media and this leads to the change from jihad to the ISIS (Laytouss, 2021, p. 3). ISIS emerged more strongly and continued armed jihad after the collapse of the Al-Qaeda group. However, the ISIS is only against other Muslims that are obstructive and do not follow Islamic teachings. ISIS uses four mechanisms to continue cyber jihad which includes: (1) globalization of jihad; (2) Utilizing geopolitical conflicts to expand networks; (3) promoting a “Virtual Caliphate” and “Electronic Jihad”; and (4) exploiting ideologically through hatred and mobilize minors that are less than 18 years old (Laytous, 2021, p. 4).

In order to achieve its objectives, the ISIS discovered cyber-jihad as an integral part of its overall strategy without the military combat and territorial takeovers. This study's first result showed that it exploited the use of social media to manipulate online networks. For instance, using the Dawn of Glad Tidings application by forming a construction that has enormous power to perform psychological warfare (Hoffman & Schweitzer, 2015). This was proven when the Kurdish Peshmerga ISIS troops conquered Mosul city. Meanwhile, this group performed a year-long online campaign about 'how people were killed and even takes their children as an example before the conquest. This method succeeded in increasing its image as an unrivaled power and affected the psychological condition of Iraq and its people (Melchior, 2014).

Furthermore, the second result showed that ISIS uses social media for recruitment opportunities by implementing different tactics to target male and female groups (Hoffman & Schweitzer, 2015). The ISIS uses images from early Islamic times of knights on horseback, battles, and glory on the battlefield featured in the organization's publications and high-quality video clips to target young men. Meanwhile, it uses "softer" images including kittens and Tumblr to target women.

ISIS also has methods of Foreign Fighters and Lone Wolf attacks to recruit and expand network (Hoffman & Schweitzer, 2015). The ISIS also relies on social media to spread its radicalization and jihadist views to encourage external volunteers from various countries to join as well as give instructions on how this is performed. Therefore, ISIS published an electronic book entitled *Hijrah* to detail how foreign volunteers can get to the caliphate. The ISIS's cyber jihad tactics encouraged the lone wolf that was inspired by the ISIS organization to perform terrorist attacks. This strategy relayed remote instructions concerning a preferred target without the need for physical communication between the perpetrator and this group member. Therefore, it operated outside the Middle East through operations and sympathetic support while performing individual terrors (Hoffman & Schweitzer, 2015).

One of the goals of cyber-jihadists through the production of radical narratives was to create propaganda. Studies such as Sharks (2010), Liang (2015), and Marone and Magri (2019) have shown that jihadists' social media activities are to conduct online messages. According to Marone and Magri (2019), propaganda is an important instrument for consolidating leadership and imposing narratives on all members and society. It also helps to preserve followers' loyalty through messages that increase morale and rationalization of provocative narratives. The tactics used included mercy, victimhood, war or the benefits of joining the military of a terror group, belongings, and utopianism that refers to the caliphate, and so on (Aly et al., 2016).

It is interesting to note that the propaganda created by cyber-jihadists has a strong relationship with violence. The ambivalent use of these online messages by terrorist groups sometimes supports or rejects violence. The frequent changes in the use of propaganda help to spread the ideology of terrorism groups (Colson, 2017). Therefore, this affects the philosophy development of individuals and collectives to commit violence considered as a logical action. Most (1885) found out that terrorist groups used propaganda as a means of

justification, systematic, tactical, and purposeful campaigns for violence. The terrorist movement was coordinated by performing martyrdom in justifying the revolution (Campion, 2015). Martyrdom is used by terrorists to form propaganda that shows heroism, glory, and reward in heaven. According to Campion (2015), this phenomenon helps to elevate the terror group as a necessary defensive measure.

Propaganda is planned in the form of acts of violence that are packaged and distributed through online media in both writing and video forms (Campion, 2015). However, the terrorist group was not only developed but there is also an improvement of online messages modus operandi by cyber-jihadists. First, Al-Qaeda led the jihad propaganda through cyberspace with the message to perform greater holy war which meant the struggle of Muslims (Heickerö, 2014). Second, ISIS is now using social media to convey messages and offering brotherhood, compensation, and caliphate in Syria (Liang, 2015). It is also using narratives including the religious obligation to become members and adventures as well as friendships with jihadists. This becomes an effort to realize the goal of mobilizing fighters and jihadist groups to join its ranks (Gartenstein-Ross & Barr, 2016). Consequently, the mobilization of Indonesian citizens to become jihadists like the ISIS is related to taking over and controlling the areas of Eastern Syria and Western Iraq that tend not to be managed effectively by the governments of Damascus or Baghdad (Sahrasad, 2017).

The third development is a significant effect in the modus operandi where there is a change in the propaganda created by ISIS. However, the ISIS succeeded in forming views among its sympathizers against the existence of taghut by using the taghut narrative (Zuhdi & Hayatullah, 2020). The Taghuts are people that make their laws because this group thinks they are higher than God. Therefore, these conditions created a rejection against the Indonesian government and led to support the ISIS. According to Dhanaraj (2018), the collapse of ISIS leads to the use of cyber jihadists to inspire more people to become lone-wolf terrorists or form smaller cell groups. This is supported by data presented by the Center for Strategic and International Studies (CSIS) that show no changes related to terror attacks in Indonesia (Nathaniel, 2021).

Propaganda is also created through extremist websites, and social media including Facebook, Twitter, and YouTube. Internet and social media platforms are among the four important assets owned by ISIS (Alkaff & Mahzam, 2018). According to Hui (2010), Blogspot sites further provide opportunities for people to read about radicalism and extremism. One Blogspot managed by Hizbut Tahrir Indonesia (HTI) has created narratives including “Jihad solves everything” and uploaded photos of firearms used by mujahideen in Afghanistan. Furthermore, the study of Armandhanu (2017) shows the photos and videos of the use of firearms and the execution of hostages uploaded by ISIS to foster a heroic attitude in their sympathizers.

The cyber-jihadists propaganda is also created through the publication of writings, studies, and radical translations that are digitized and accessed by various platforms. For instance, Aman Abdurrahman spreads radicalism through his blog namely millahiibrahim.blogspot.com. Bahrn Naim uses blogs like www.bahrnaim.co, www.bahrnaim.site, and www.bahrnaim.space, to spread radical ideas and provide manual instructions how to execute terrorist activities (Rozika, 2017). Therefore, the shift in the propaganda narrative is an effort to spread the ISIS alliance to various regions of the world. This change has helped to develop a political methodology of the ISIS. These online messages enable ISIS to speak to everyone in the world by calling for the mobilization and support needed in winning the religious war. Furthermore, propaganda offers its

sympathizers the religious truth, Muslim collective consciousness, adventure, the opportunity to feel strong, and take refuge. ISIS emphasizes the international Muslims to perform jihad as an obligation to fight threats to Islam through these messages and narratives (Orozobekova, 2016).

Cyber-Jihadist as Rational Choice

In Indonesia, the cyber jihadist is developed by ISIS and this is indicated with the use of the media as a means of disseminating radical ideology. For instance, Aman Abdurrahman encouraged his followers to join ISIS through translations, writings, and sermons remade. These messages were disseminated by social media platforms including Facebook, Twitter, and YouTube (Sahasrad, 2020). According to Sahasrad (2020), 9 out of 14 radical websites originated from the Indonesian domain from where the ISIS flag promotes Islamic law and the caliphate, as well as counters negative news narratives.

Hui (2010) explained that the narrative of radical websites in Indonesia is the use of social media. There are several characteristics of radical websites including an injustice against the Muslim community in the Middle East. The content of these narratives expands and focuses on the situation in undocumented countries including Southern Thailand and the Maldives where persecution occurs against Islam. The injustices against Muslims in other parts of the world have prompted sentiments of moral outrage. Generally, the post-911 jihadi movement becomes a source of radical sentiment and this help to create a new narrative especially in Indonesia where there is a local contextualization of global discourse. Furthermore, the study of Hui (2010) showed the solidarity of online radicals with their "compatriots".

The relationship between local and global terror groups was built-in communication and this helps Indonesian citizens to migrate to Syria. Recently, the connection between cyber-jihadists and network groups is in the form of verses, hadith, and news, as well as knowledge support in performing terror activities including bomb-making and technology use drones. According to FTF Task Force (2020), all information support is performed through communication platforms such as WhatsApp, Telegram, or Discord groups. Furthermore, the terror attack in another country or the conquest of territory in Syria enable the cyber-jihadists to amplify the news and motivate terror groups in Indonesia.

Choi et al. (2018) emanated the discussion of rational choice including cyberterrorism to the latest terrorism phenomenon. The study focused on aspects of cyberterrorism with the use of technology or resources by terrorists. In another study, Guerette and Santana (2010) posited that the RCT shows how to exploit technology for group or individual calculations, as well as to predict the risks and benefits associated with the type of attack chosen.

Reduced risk, effort to use technology, and reward for motivation are three components that affect an individual's decision to commit cyberterrorism as a rational action (Choi et al., 2018). The first component of RCTs in cyberterrorism is the principle of reduced risk which leverages cyber resources. The second principle is effort related to technological facilities and presence that is not too risky. However, easy access to potential targets online suggests there are no limits to terrorists' physical presence. Terror groups directly upload unedited videos of attacks or propaganda for mass audiences by using the internet. The third component of reward is related to terrorist motivation. For instance, the enhancement of the terror group's reputation within subcultural helps to hide their real identity and falsify physical location (Choi et al., 2018). Thus, Choi et al. (2018) look at factors that are considered by the perpetrators in becoming a cyber-jihadist. These factors stem from the study of Cornish and Clarke (1986) on the rational choice structure.

The interviews with five informants revealed seven points shown in Table 4:

Table 4 Rational Choice Structure in Indonesian *Cyber-Jihadist*

No.	Rational Choice Structure	Informants				
		AVR	WA	AH	MS	RW
1.	<i>Availability</i>	✓	✓	✓	✓	✓
2.	<i>Awareness of method</i>	✓	✓	✓	✓	✓
3.	<i>Likely cash yield per crime</i>	-	-	-	-	-
4.	<i>Expertise needed</i>	✓	✓	✓	✓	✓
-5.	<i>Planning necessary</i>	-	-	-	-	-
6.	<i>Resources required</i>	✓	✓	✓	✓	✓
7.	<i>Solo versus assistance required</i>	-	-	-	-	-
8.	<i>Time required to commit</i>	✓	✓	✓	✓	✓
9.	<i>Cool nerves required</i>	-	-	-	-	-
10.	<i>Risk of apprehension</i>	-	✓	✓	✓	✓
11.	<i>Severity of punishment (if caught)</i>	-	-	-	-	-
12.	<i>Instrumental violence required</i>	-	-	-	-	-
13.	<i>Confrontation with victim</i>	-	-	-	-	-
14.	<i>Identifiable victim</i>	-	-	-	-	-
15.	<i>Social cachet</i>	-	-	-	-	-
16.	<i>Fencing necessary</i>	-	-	-	-	-
17.	<i>Moral evaluation</i>	✓	✓	✓	✓	✓

Table 4 shows 7 points of the rational choice structure including availability, method awareness, expertise needed, resources required, the time required to commit, risk of apprehension, and moral evaluation are fulfilled. These points are the basis for considering the cyber jihadists perpetrators.

According to Cornish and Clarke (1986), availability is related to easy access in committing crimes. Therefore, perpetrators are faced with three choices including becoming terrorists in Indonesia, participating in jihad in Syria, and creating propaganda and supporting terror activities on social media and telecommunications platforms. Five participants revealed that the third choice was the easiest and most likely option needed to be chosen. This was because internet access was very easy to get and their free time enabled them to discuss with others, find information, and spread it to social media. According to rational choice, the perpetrators were willing to take their time in committing crimes (Mandelcorn et al., 2013).

The study of Cornish and Clarke (1986) showed that method awareness was the perpetrators' understanding of the tactics used in committing their crimes. Subsequently, the context of cyber-jihadists indicated that the internet, operating social media, and sending

information to telecommunication groups were the only knowledge needed. This is in line with the study of Cavelti and Balzacq (2018) that the cyber-terrorism method is easy to use by terrorists because there are so many systems and technologies based on open-source. Meanwhile, the perpetrators had a social media account before joining the terror group for a long time. All informants made their allegiance to Abu Bakr Al Baghdadi the ISIS leader and also showed their awareness about this group and other groups like the Daulah Islamiyah through the internet. Therefore, all the participants had the required information and skills needed to become cyber-jihadists.

According to the informants, special techniques were not required to become a cyber-jihadist because it was very easy to do so. The participants explained that the terrorist activities they just committed were performed by people with social media accounts or telecommunication platforms including WhatsApp and Telegram. All these informants used the same mode of transmission but distributed different messages. The perpetrators spread content and information about ISIS, while others shared and discussed politics, entertainment, and other social issues. According to Vacca (2019), the use of social media in terrorism is easy without any special training and it also helps to reduce the costs needed to perform similar activities offline.

In cyber-jihad, there are no special tools needed to commit crimes because all the informants used only Android phones to create propaganda, disseminate information, initiate Facebook, Telegram, and WhatsApp groups. According to the participants, few people used cellphones, computers, or laptops to carry out their terrorist activities but mobile phones and the internet were the main tools used by cyber-jihadists. Choi et al. (2018) showed that the perpetrators of cyber terrorism did not need great effort to register their presence in a certain place while committing the crime. The internet facilitated all the needs to upload, download, or disseminate the desired content by using simple equipment (Choi et al., 2018).

Furthermore, there is no limited time for cyber jihadists to commit crimes or perform any terrorist activities. According to Jaishankar (2008), the crimes committed in cyberspace do not have a time limit because cyberspace is an ideal place for criminals to perform their actions. His study showed that cyber-jihadist activities were performed during working hours, breaks, and while at home. Moreover, propaganda was created simultaneously with other tasks including watching television or gathering with friends and family. The cyber jihadists did not feel burdened with the spreading of messages because they had the freedom of managing time.

The current study considered the risk of apprehension because the crimes committed would affect the informants' rational choice to become cyber-jihadists. The participants made this decision because they felt it was safer by taking cover behind the anonymity in cyberspace. According to Akdeniz (2002), internet technology allowed anonymous communication for useful and criminal purposes. Furthermore, anonymity was associated with cybercrime and this meant it allowed terrorists to perform criminal activities without the possibility of being detected (Akdeniz, 2002). The use of anonymous names or vague usernames on various social media platforms reduced the risk of being arrested. In contrast, AVR did not consider the risk of being apprehended because this informant did not know that its actions in disseminating information and being an admin in ISIS-affiliated social media groups were a form of crime.

Another point fulfilled in this study was a moral evaluation that is related to the difference between good and bad behavior or feelings of right and wrong due to one's conscience as a human being. According to most informants' conscience as a true Muslim, it is good and

right to become a jihadist. However, ISIS is a strong magnet for Muslims around the world to swear allegiance and emigrate because it declared the Khilafah. This declaration attracted the sympathy of Islam followers around the world to join and fight with ISIS (Mbai, 2014). The act of being a cyber-jihadist is an actualization in preaching the "good news" about the caliphate proclaimed by the ISIS. Furthermore, being a cyber-jihadist rationally and consciously was an attempt to complete their jihad obligations as a Muslim.

The informants explained that becoming cyber-jihadists was the most feasible choice compared to joining jihad in Syria and performing terror acts in Indonesia. Meanwhile, the participants discussed that large capital was needed in migrating to Syria but small funds were required to become cyber-jihadists in your own country. According to the Bipartisan Policy Center (2018), technological developments with the emergence of social media help terrorist groups to spread propaganda and recruit new members anywhere and at no cost. Furthermore, several communication platforms help to provide free encrypted messages that can be used without any regional or user restrictions (Bipartisan Policy Center, 2018).

Conclusion

The development of the internet is heavily used and exploited by terrorists to promote the violent idea of 'jihad' against the enemies of Islam. This phenomenon is used by two major terror groups including Al-Qaeda and ISIS to create propaganda, recruitment, communication, fundraising, attack preparation, and others. However, jihad is called cyber-jihad because it uses the internet in spreading messages. In Indonesia, the cyber-jihadist is developed by ISIS and this is indicated with the use of the media as a means of disseminating radical ideology. This study has used rational choice theory to discover the creation of propaganda, disseminate information related to ISIS and radicalism, as well as fundraising for online terror activities. Therefore, terrorist actions become rational despite being considered as irrational.

Several scientists have attempted to include a rational framework to enable the community to understand traditional terrorism. According to Choi et al. (2018), terrorism in cyberspace is the recent one that terrorist groups normally venture into. The study identified several components of RCTs including the lower risk for perpetrators, easy effort and access to potential targets, as well as terrorist motivation for better rewards in cyberterrorism. Following the recommendations of Cornish and Clarke (1986), this study used the rational choice structure which contained seventeen points to develop an analysis of the cyber-jihadist in Indonesia.

The interviews with five informants showed that there were seven points more pertinent out of this list of seventeen: availability related to easy access and free time from the participants; method awareness such as internet and social media to send information about ISIS; expertise needed to become a cyber-jihadist; required resources and tools; time needed to commit a crime; less risk and fear of being caught as a cyber-jihadist due to anonymity; and moral evaluation by a true Muslim to be a jihadist.

The informants also revealed that following their voice of their conscience, as a true Muslim, they had become a jihadist. ISIS though proved a strong magnet which attracted the sympathy of Islam followers around the world to join and fight with ISIS. This was the making of a cyber-jihadist rationally and consciously. This study thus justified the use of the rational framework to understand the cyber-jihadist phenomenon in Indonesia. It succeeded in analyzing the perpetrators' rationality to decide in becoming a cyber-jihadist using rational choice theory.

References

- Akdeniz, Y. (2002). Anonymity, democracy, and cyberspace. *Social Research: An International Quarterly*, 69(1), 223-237. <https://muse.jhu.edu/article/557276>
- Akers, R. L. (1990). Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken. *Journal of Criminal Law and Criminology*, 81(3), 653-676. <https://scholarlycommons.law.northwestern.edu/jclc/vol81/iss3/6>
- Alkaff, S. H. B. O., & Mahzam, R. (2018). Islamic state after the fall of Mosul and Raqqa. *Counter Terrorist Trends and Analyses*, 10(1), 57-61. <https://www.jstor.org/stable/26349856>
- Aly, A., Macdonald, S., Jarvis, L., & Chen, T. (2016). *Violent Extremism Online: New Perspectives on Terrorism and the Internet*. Taylor & Francis. <https://books.google.com.pk/books?id=hN8eDAAAQBAJ>
- Ansori, M. H. (2019). *Membertantas terorisme di Indonesia: praktik, kebijakan dan tantangan*. Habibie Center.
- Badan Nasional Penanggulangan Terorisme (BNPT). (2016). *Strategi Menghadapi Paham Radikalisme Terorisme-ISIS*. Jakarta: Belmawa. <https://www.academia.edu/download/54852192/Strategi-Menghadapi-Paham-Radikalisme-Terrorisme.pdf>
- Basit, A. (2020). COVID-19: a challenge or opportunity for terrorist groups? *Journal of Policing, Intelligence and Counter Terrorism*, 15(3), 263-275. <https://doi.org/10.1080/18335330.2020.1828603>
- Bipartisan Policy Center. (2018). *Digital counterterrorism: Fighting jihadists online*. Washington DC: Task Force on Terrorism and Ideology.
- Campion, K. K. (2015). *Under the Shadows of Swords: Propaganda of the Deed in the History of Terrorism*. [Thesis (PhD)]. James Cook University. <https://researchonline.jcu.edu.au/48293/>
- Campos, N. F., & Gassebner, M. (2009). International terrorism, political instability and the escalation effect. *CEPR Discussion Paper No. DP7226*. <https://ssrn.com/abstract=1372546>
- Caplan, B. (2006). Terrorism: The relevance of the rational choice model. *Public Choice*, 128(1), 91-107. <https://doi.org/10.1007/s11127-006-9046-8>
- Cavelty, M. D., & Balzacq, T. (2018). *Routledge Handbook of Security Studies*. Routledge. <https://books.google.com.pk/books?id=-FrztgEACAAJ>
- Choi, K.-s., Lee, C. S., & Cadigan, R. (2018). Spreading propaganda in cyberspace: Comparing cyber-resource usage of Al Qaeda and ISIS. *International Journal of Cybersecurity Intelligence & Cybercrime*, 1(1), 21-39. <https://www.doi.org/10.52306/01010418ZDCD5438>
- CNN Indonesia. (2018). Pemimpin ISIS Al-Baghdadi Serukan Jihad dalam Idul Adha. <https://www.cnnindonesia.com/internasional/20180823072622-120-324227/pemimpin-isis-al-baghdadi-serukan-jihad-dalam-pesan-idul-adha>
- Colson, D. (2017). Propaganda and the deed: Anarchism, violence and the representational impulse. *American Studies*, 55(4), 163-186. <https://www.jstor.org/stable/44982624>
- Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Transaction Publishers. <https://books.google.com.pk/books?id=VfmmAgAAQBAJ>
- Crenshaw, M. (1981). The causes of terrorism. *Comparative politics*, 13(4), 379-399. <https://doi.org/10.2307/421717>

- Davis, B. R. (2006). Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance. *CommLaw Conspectus*, 15, 119-186. <https://scholarship.law.edu/cgi/viewcontent.cgi?article=1353&context=commlaw>
- Dhanaraj, J. (2018). Evolution of the Islamic State After its Territorial Defeat. *Counter Terrorist Trends and Analyses*, 10(5), 1-7. <https://www.jstor.org/stable/26435152>
- Emina, K. A., & Ikegbu, E. A. (2020). The role of the military to national development in Nigeria. *socialspacejournal.eu*, 20(2), 185-208. [http://socialspacejournal.eu/Social%20Space%20Journal%202020\(20\).pdf#page=185](http://socialspacejournal.eu/Social%20Space%20Journal%202020(20).pdf#page=185)
- Gartenstein-Ross, D., & Barr, N. (2016). *The Islamic State's global propaganda strategy*. JSTOR. <https://www.jstor.org/stable/pdf/resrep29413.pdf>
- Guerette, R. T., & Santana, S. A. (2010). Explaining victim self-protective behavior effects on crime incident outcomes: A test of opportunity theory. *Crime & Delinquency*, 56(2), 198-226. <https://doi.org/10.1177%2F0011128707311644>
- Haykel, B. (2016). ISIS and al-Qaeda—what are they thinking? Understanding the adversary. *The ANNALS of the American Academy of Political and Social Science*, 668(1), 71-81. <https://doi.org/10.1177%2F0002716216672649>
- Heickerö, R. (2014). Cyber terrorism: Electronic jihad. *Strategic Analysis*, 38(4), 554-565. <https://doi.org/10.1080/09700161.2014.918435>
- Hoffman, A., & Schweitzer, Y. (2015). Cyber jihad in the service of the Islamic State (ISIS). *Strategic assessment*, 18(1), 71-81. <https://www.inss.org.il/publication/cyber-jihad-in-the-service-of-the-islamic-state-isis/>
- Hui, J. Y. (2010). The internet in Indonesia: Development and impact of radical websites. *Studies in Conflict & Terrorism*, 33(2), 171-191. <https://doi.org/10.1080/10576100903400605>
- Iskandar, O. M. A. (2020). Menebar konten membendung radikalisme. <https://www.antaraneews.com/berita/1814497/menebar-konten-membendung-radikalisme>
- Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmallegger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Pearson. <https://www.researchgate.net/publication/321716315>
- Joffroy, S. (2020). Un Master unique en France. *Res Militaris*, 10(2), 1-7. <https://resmilitaris.net/index.php/2020/06/01/id1032027/>
- Junaid, H. (2013). Pergerakan Kelompok Terorisme dalam Perspektif Barat dan Islam. *Sulesana: Jurnal Wawasan Keislaman*, 8(2), 118-135. <https://doi.org/10.24252/.v8i2.1285>
- Karjo, C. H., & Ng, A. (2020). Hate Speech Propaganda from and against Muslims in Facebook Posts. *International Journal of Cyber Criminology*, 14(2), 400-416. <http://dx.doi.org/10.5281/zenodo.4766989>
- Kominfo.go.id. (2019). Kominfo Blokir 11.803 Konten Radikalisme dan Terorisme Siaran Pers No. 63/HM/Kominfo/03/2019. https://kominfo.go.id/content/detail/17274/siaran-pers-no-63hmkominfo032019-tentang-kominfo-blokir-11803-konten-radikalisme-dan-terorisme/0/siaran_pers
- Korbl, W. (2017). Terrorism: Motivation and Theory. *The Journal of Public and Professional Sociology*, 9(2), 1. <https://digitalcommons.kennesaw.edu/jpps/vol9/iss2/1>

- Kurniawan, A. R., & Primawardani, Y. (2019). Proporsionalitas Pembatasan Ham Dalam Pasal 28 Undang-undang Pemberantasan Tindak Pidana Terorisme. *Jurnal Legislasi Indonesia*, 16(1), 16–26. <https://doi.org/10.54629/jli.v16i1.449>
- Kydd, A. H., & Walter, B. F. (2006). The strategies of terrorism. *International security*, 31(1), 49–80. <https://doi.org/10.1162/isec.2006.31.1.49>
- Liang, C. S. (2015). Cyber Jihad: understanding and countering Islamic State propaganda. *GSCP Policy Paper*, 2(4), 1–12. <https://www.files.ethz.ch/isn/189426/2015%20%20Cyber%20Jihad.pdf>
- Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press. <https://books.google.com.pk/books?id=QUYMwJR5pYMC>
- Mandelcorn, S., Modarres, M., & Mosleh, A. (2013). An Explanatory Model of Cyber-Attacks Drawn from Rational Choice Theory. *Transactions of the American Nuclear Society*, 109(1), 1869–1871. <https://www.ans.org/pubs/transactions/article-22132/>
- Marone, F., & Magri, P. (2019). *Digital Jihad: Online Communication and Violent Extremism*. Ledizioni LediPublishing. <https://books.google.com.pk/books?id=m2DNDwAAQBAJ>
- Mbai, A. (2014). *Dinamika Jejaring Teror di Indonesia*. Jakarta: AS. Production Indonesia.
- Nalbandov, R. (2013). Irrational rationality of terrorism. *Journal of Strategic Security*, 6(4), 92–102. <https://www.jstor.org/stable/26466751>
- Nathaniel, S. P. (2021). Ecological footprint, energy use, trade, and urbanization linkage in Indonesia. *GeoJournal*, 86(5), 2057–2070. <https://doi.org/10.1007/s10708-020-10175-7>
- Nemeth, C. P. (2017). *Private security and the law*. CRC Press. <https://doi.org/10.1201/9781315184449>
- Oberschall, A. (2006). *Vojislav Seselj's nationalist propaganda: Contents, techniques, aims and impacts, 1990–1994*. An expert report for the United Nations International Criminal Tribunal for the former Yugoslavia. https://www.baginst.org/uploads/1/0/4/8/10486668/vojislav_seseljs_nationalist_propaganda-contents-techniques-aims-and-impacts.pdf
- Orozobekova, A. (2016). The Mobilization and Recruitment of Foreign Fighters: The Case of Islamic State, 2012–2014. *Connections: The Quarterly Journal*, 15(3), 83–100. <https://doi.org/10.11610/Connections.15.3.07>
- Pape, R. A. (2003). The strategic logic of suicide terrorism. *American political science review*, 97(3), 343–361. <https://doi.org/10.1017/S000305540300073X>
- Rozika, W. (2017). Propaganda dan Penyebaran Ideologi Terorisme Melalui Media Internet (Studi Kasus Pelaku Cyber Terorisme oleh Bahrun Naim). *Jurnal Ilmu Kepolisian*, 11(2), 122–134. <http://www.jurnalptik.id/index.php/JIK/article/view/89>
- Sahasrad, H. (2017). ISIS, INDONESIAN MUSLIMS AND GLOBAL TERRORISM: A REFLECTION. *JICSA (Journal of Islamic Civilization in Southeast Asia)*, 6(1), 59–91. <https://doi.org/10.24252/jicsa.v6i1.4230>
- Sahasrad, H. (2020). A'an Suryana. The State and Religious Violence in Indonesia: Minority Faiths and Vigilantism. *Center for Southeast Asian Studies, Kyoto University*, 9(1), 131–134. https://doi.org/10.20495/seas.9.1_131
- Sanur, D. (2018). Terorisme: Pola Aksi dan Antisipasinya. *Bidang Pemerintahan dalam Negeri Kajian Singkat terhadap Isu Aktual dan Strategis*, 10(10), 25–30. https://berkas.dpr.go.id/puslit/files/info_singkat/Info%20Singkat-X-10-II-P3DI-Mei-2018-212.pdf

- Sari, B. D. A. C. (2017). Literacy Media in The Counter of Radicalism Propaganda and Terrorism Through Internet Media. *Jurnal Prodi Perang Asimetris*, 3(1), 15-31. <https://jurnalprodi.idu.ac.id/index.php/PA/article/view/91>
- Sarinastiti, E. N., & Vardhani, N. K. (2018). Internet dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism New Media. *Jurnal Gama Societa*, 1(1), 40-52. <https://journal.ugm.ac.id/jgs/article/viewFile/34048/20303>
- Shehata, S. (2015). Threats of MoDerN terrorist orGaNizationNs aND state spoNsoreD terrorisM—the case of islaMic state. *Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje*(19), 216-233. <https://kulturabezpieczenstwa.publisherspanel.com/resources/html/article/details?id=176580>
- Shughart, W. F. (2011). Terrorism in Rational Choice Perspective. In C. J. Coyne & L. Rachel (Eds.), *The Handbook on the Political Economy of War*, Cheltenham, UK and Northampton (pp. 126-153). Edward Elgar Publishing. <https://doi.org/10.4337/9781849808323.00015>
- Simons, G., & Cristina, B. (2020). The Specter of Terrorism During the Coronavirus Pandemic. *E-International Relations*, 1-3. <https://www.e-ir.info/2020/05/08/the-specter-of-terrorism-during-the-coronavirus-pandemic/>
- Suard, I. G. W. (2020). Challenges of Implementing Deradicalisation Programs for Terrorist Prisoners: An Examination of Indonesian Prison Officers' Experiences. *International Journal of Criminal Justice Sciences*, 15(2), 173-190. <http://dx.doi.org/10.5281/zenodo.3830309>
- Vacca, J. R. (2019). *Online terrorist propaganda, recruitment, and radicalization*. CRC Press. <https://doi.org/10.1201/9781315170251>
- van Um, E. (2015). *Evaluating the Political Rationality of Terrorist Groups*. Springer Fachmedien Wiesbaden. <https://books.google.com.pk/books?id=tvrrpCgAAQBAJ>
- Zuhdi, M. L., & Hayatullah, I. K. (2020). NARRATIVE FOR TERRORISM AND TRANSNATIONALISM ISISTHEOLOGY THROUGH THE DOCTRINE OF RELIGION. *Journal of Terrorism Studies*, 2(1), 20-31. <https://doi.org/10.7454/jts.v2i1.1015>