Cyber-Terrorism in the Context of *Proselytizing, Coordination, Security,* and *Mobility*

Iqbal Ramadhan

Affiliation: International Relations Department of Universitas Pertamina
Email: iqbal.ramadhan@universitaspertamina.ac.id

Abstract

The simplicity and flexibility of information and technology have made human life more comfortable. Terrorist groups have been using these things to disseminate terror, recruit new members, fundraise, and mobilize their activities. Technology provides the terrorist group an exploit to conduct its hideous activity. Globalization eventually gives the double-edged sword that needs to be addressed by state actors regarding terrorist issues. The author used James D. Kiras' four cyber-terrorism concepts: proselytizing, coordination, security, and mobility. The terrorist group harnesses those four concepts in the modern world to achieve their interest. On the other side, the author harnessed comprehensive security from the Copenhagen School of Security Studies to analyze cyber-terrorism activity threats. This article aims to analyze terrorist groups in conducting their activity based on Kiras' four cyber-terrorism concepts. Using Kiras' concept and Comprehensive Security from Copenhagen School, the author aims to analyze the impact of cyber terrorism on society and prevent such a threat. The author also used the qualitative method as an analytical tool to analyze the research problem and concluded that states had to establish a rigid counter-terrorism system holistically at the domestic level without neglecting international strategic cooperation among international actors to counter this threat.

Keywords: Cyber-terrorism, proselytizing, coordination, security, mobility.

Abstrak

Kesederhanaan dan fleksibilitas informasi dan teknologi membuat kehidupan manusia semakin nyaman. Kelompok teroris telah menggunakan hal-hal ini untuk menyebarkan teror, merekrut anggota baru, menggalang dana, dan

memobilisasi aktivitas mereka. Teknologi memberikan kelompok teroris suatu eksploitasi untuk melakukan aktivitas mengerikannya. Globalisasi pada akhirnya memberikan pedang bermata dua yang perlu disikapi oleh para aktor negara terkait isu teroris. Penulis menggunakan empat konsep cyber-terorisme James D. Kiras: dakwah, koordinasi, keamanan, dan mobilitas. Kelompok teroris memanfaatkan keempat konsep tersebut di dunia modern untuk mencapai minat mereka. Di sisi lain, penulis memanfaatkan keamanan komprehensif dari Copenhagen School of Security Studies untuk menganalisis ancaman aktivitas cyber-terrorism. Artikel ini bertujuan untuk menganalisis kelompok teroris dalam melakukan aktivitasnya berdasarkan empat konsep cyber-terorisme Kiras. Menggunakan konsep Kiras dan Keamanan Komprehensif dari Sekolah Kopenhagen, penulis bertujuan untuk menganalisis dampak terorisme dunia maya terhadap masyarakat dan mencegah ancaman semacam itu. Penulis juga menggunakan metode kualitatif sebagai alat analisis untuk menganalisis masalah penelitian dan menyimpulkan bahwa negara harus membangun sistem kontra-terorisme yang kaku secara holistik di tingkat domestik tanpa mengabaikan kerja sama strategis internasional di antara para aktor internasional untuk melawan ancaman ini.

Kata kunci: *Cyber-terrorism, dakwah, koordinasi, keamanan, mobilitas.*

INTRODUCTION

The problem regarding security in a cyber-world does not only involve technical, hardware, or software issues. Furthermore, it drags interstate relations between one country and another. Joseph S.Nye (2011) once said in his book, *The Future of Power*, that states must have the ability to rule technological power because the cyber-world provides another threat. Human in the modern world cannot ignore their dependence on technology. As one of world politics's main actors, even states heavily depend on technology to sustain their critical sectors such as defense, governance, finance, and energy. As once stated by Kshetri (2014), the state's security and relations involve both physical and cyber aspects. It means that states must overcome threats that are coming from the cyber-world. Myriam Dunn Cavelty emphasized that cyber threat always correlates with national security (Cavelty in Mauer and Cavelty, 2010). Hence,

protecting national cybersecurity is essential for maintaining political, social, and economic stability.

As a new issue in security studies, cyber threat is not a bluffing nor a myth. A prominent institution such as Pricewaterhouse Cooper (PwC) Global, in 2013, conducted some research and analyzed that the number of cyberattacks would increase each year. The cyber-world attack had significantly increased to 23 percent at that time (PwC, 2014). Indeed, those numbers were not static but dynamic. They said that technology eventually would improve and become more sophisticated. It has also made some causality in which the cyber attack would be more advance (PwC, 2014). How about the cyberattack in 2018? Was there any escalation? Forbes made a forecast that the attack would involve a terrorist group. Forbes said the terrorist could exploit a vulnerability in states' internet backbone like the financial and banking sector. In 2015, the Cyber Caliphate, linked to ISIS (Islamic State of Iraq and Syria), hacked and stole 1,000 US military defense (Gilsinan, 2018). Meanwhile, in 2013, approximately 6,000 Indonesia's IP addresses had been infiltrated by malware and virus to steal essential data (ID-CERT, 2013).

Cyber threat typologies come from different types. For example, Myriam Dunn Cavelty divides it into three typologies: *cybercrime*, *cyberwar*, and *cyber-terrorist* (Cavelty in Mauer and Cavelty, 2010). Cybercrime is placing a criminal organization's ability to harness and cover their crime activity using technological sophistication. On the other side, cyberwar is a digital version of Von Clausewitz's war where technology specializes in modern warfare. The third one is cyber-terrorism, where terrorist groups exploit the technological advantage to spread fear for political purposes and destabilize national security (Cavelty in Mauer and Cavelty, 2010). Cavelty's typology is slightly different from Jonathan D. Aronson's argument. He said that cyber threats came in intelligence gathering, hacking, and cyberwar (Aronson in Bayliss, 2005). Aronson explained that intelligence gathering tends to come in the act of cyber spying activity. Meanwhile, hacking has the purpose of stealing important data, and cyberwar emphasizes state defense capability using technological advancement to cripple its opponent (Aronson in Bayliss, 2015).

The author will focus on cyber-terrorism as the central issue in this article. From the author's perspective, there is no firm definition regarding what cyber-terrorism is. However, several types of research were trying to define the activity of cyber-terrorism. One of them is a study conducted by Michael L. Gross, Daphne Canetti, and Dana R. Vashdi called *Cyber-terrorism: Its Effect on Psychological Well-being, Public Confidence, and Political Attitudes*. Their study discussed cyber-terrorism's impact on human psychology (Gross, Canetti, and Vashdi, 2017). They used quantitative methodology to quantify and measure human psychology after watching videos on terrorist recruitment, propaganda, or their diabolical activities (Gross, Canetti and Vashdi, 2017). From their argument, cyber-terrorism is an act of terrorism by harnessing malware and even media information systems to recruit a new member and destabilize state national security (Gross, Canetti and Vashdi, 2017).

Another research has other definitions to describe cyber-terrorism. That activity can be defined as an act of violence to spread fear among citizens by using information systems and influence public opinion towards national security (Samuel and Osman, 2014). Kobuye Oluwafemi Samuel and Wan Rozaini Sheik Osman, in their journal, *Cyber-terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences, and Panacea*, were focusing their research on military defense system and its impact on state defense capability. How does the terrorist group take advantage of modern technology to achieve its purpose? Myriam Dunn Cavelty stated that cyber-terrorism is an easy method for a terrorist to utilize because many technological systems are open source based. Hence, most people, including the terrorist group, can use it to exploit a state's information system (Cavelty in Mauer and Cavelty, 2010). On the other hand, Joseph S. Nye disagreed that terrorist groups can cripple its backbone. He argued that it would be possible for them to exploit the state's information system (Nye, 2011).

Cyber-terrorism can target everyone to show and demonstrate the terrorist's political purpose. For example, ISIS once targeted 19,000 France multinational companies, universities, and government websites to protest Prophet Muhammad's defamation

by Charlie Hebdo. They defaced the user interface and changed it by putting terrorist propaganda (Giantas & Stergiou, 2018). Another case had shown that a young man from Kosovo who had an affiliation with ISIS was proven guilty because he hacked a considerable amount of US Army personnel data (Federal Times, 2016). Terrorist groups like ISIS also disseminated *kill lists* containing personal information from twenty-two (22) US departments. They would use it to order *sleeper cells* (ISIS hidden agents) worldwide to execute whoever is on that list (Giantas & Stergiou, 2018).

Indonesia, as the largest Muslim country, indeed cannot ignore this kind of new threat. Cyberspace is no longer a haven since terrorist uses it to recruit new members or gains funding to support their cause. One research indicated that terrorist is targeting young people and harnessing "new media" like Facebook, Twitter, and Youtube (Sarinastiti & Vardhani, 2018). The terrorist knew that the new social media platform is the perfect medium to gain influence and recruit its supporters (Sarinastiti & Vardhani, 2018). Instead of crippling the nation's state IT system, terrorist groups are far more dangerous by recruiting and gaining support through social media (Sarinastiti & Vardhani, 2018). Cyberspace or internet is easy to access and terrorist exploits it quickly due to its security, mobility, accessibility, and the ability to reach a wider audience (Bambang & Fitriana, 2017). By reaching its spectators, they will brainwash, recruit, and spread its radical ideology in Indonesia's moderate Muslim citizens (Bambang & Fitriana, 2017). Another research showed a shred of evidence that most terrorist groups are recruiting Indonesian young people through social media like Facebook, Twitter, and Youtube (Lubis, 2017). This research indicated that young people were vulnerable since they were volatile and easy to influence due to their immature behavior (Lubis, 2017). Based on Badan Nasional Penanggulangan Terorisme (BNPT) or Indonesia National Agency for Terrorist Prevention, approximately 4 percent of Indonesia's citizens pledge their support to ISIS (Putri, 2019). They also had deradicalized 500 ex-ISIS combatants who held an Indonesian passport from 2017-2019 (Putri, 2019).

The main focus of this article will be cyber-terrorism and its impact on nation-state stability and security. States have to protect

their national stability and their people to anticipate the upcoming threat. The stepping stone of this problem came from James D. Kiras' concept of cyber-terrorism in the modern world, such as *proselytizing*, *coordination*, *security*, and *mobility* (Kiras in Bayliss et al., 2014). The author used the Kiras' central concept to analyze the threat and a referent object. First, states have to identify who will be threatened by cyber-terrorism because it affects plenty of referent objects, ranging from state, multinational company, society, and even on an individual level. As the main actor in international relations, states are responsible for protecting their political stability and their people's safety. From those concepts, the author initiates a research question: **"how does the state prevent the threat of cyber-terrorism based on the concept of proselytizing, coordination, security, and mobility?"** The author will use qualitative methods and the Copenhagen School of Security Studies relevant to International Relations Studies. This article aims to analyze how terrorist groups conduct their cyber-terrorism activity from the concept of proselytizing, coordination, security, and mobility.

Conceptual Framework

The author used Kiras' concept of cyber-terrorism to analyze the research question above. Proselytizing can be defined as a terrorist group's effort to recruit new members, gain sympathy, and fundraising (Kiras in Bayliss et al., 2014). The outcome of technology, such as social media, is a perfect medium for disseminating terrorist ideology. Most of them, such as ISIS, used social media like Facebook, Youtube, and even Twitter to recruit new members. Kiras said that this technique is efficient, especially in the Middle East (Kiras in Bayliss et al., 2014). As in coordination, terrorist groups harness the flexibility of technology to coordinate among the internal members. Nowadays, technology has provided most people to connect easily. People are familiar with chatting applications such as email, Line, or Telegram, embedded in the smartphone. Kiras stated that terrorist groups such as Al-Qaeda had done this MO (Modus Operandi) to launch an attack on September 11th, 2001 (Kiras in Bayliss, 2014).

Technology has given another benefit to the terrorist group. Even though a technological product is flexible to use, most hardware and software are more secure from time

to time. As we can say, most system developers have upgraded their software and hardware application with encryption. Eventually, terrorist groups can communicate anonymously and have no fear of being tapped by a third party (Kiras in Bayliss, 2014). Nevertheless, this technology security affects terrorist mobility. For example, terrorist groups can now implement covert missions and have the opportunity to mobilize from one country to another (Kiras in Bayliss et al., 2014). Preventing the impact of cyber-terrorism needs to be done by a nation-state to protect their sovereignty.

The author utilized the concept of security studies from Copenhagen School as a tool of analysis for analyzing and mitigating the threat of cyber-terrorism. From this conceptual framework, the author used *comprehensive security* to define the state's ability to resolve the threat that can change states' integrity and identity (Buzan, 1991). Security studies were developed by Barry Buzan, Ole Wæver, and Jaap Wilde to comprehend traditional and non-traditional security. The author employed security concepts such as threat, vulnerability, referent object, and security sector to understand cyber-terrorism as a threat (Buzan et al., 1998: 7-11). Buzan defined threat as something or someone who can hinder a state, organization or individual from obtaining their primary goals (Buzan et al., 1998: 7-11). Buzan also explained the referent object as an object threatened by incoming threat (Buzan et al., 1998: 7-11). He argued that every referent object would be different depending on its sector. Buzan classified five security sectors: military, economics, societal, political, and environmental (Buzan et al. 7-11). Every sector has its threat, which means referent objects can differ from one another (Buzan et al., 1998: 7-11). On the other hand, Buzan also explained vulnerability as the incapability of state, organization, or individual to overcome and tackle the threat (Buzan et al., 1998: 7-11). The author combined both Kiras' concept of cyber-terrorism and security studies to analyze threats and their impact on the referent objects and how states should respond to the threat.

Proselytizing

In the previous chapter, the author mentioned that proselytizing is a technique or method for disseminating terrorist ideology, recruiting new members, and fundraising by using technology.

The purpose of proselytizing intends to nurture and sustain the existence of supporters of the group's revolution. One of the easiest ways to proselytize is using social media, which is accessible and user-friendly among people in this modern world. Rand Corporation researched social media's impact on disseminating radical ideology and recruiting new terrorist members. For example, ISIS successfully mobilized its 40,000 sympathizers, promoting and gaining influence through social media (Ward, 2018). Majid Alff, Parisa Kaghazgaran, and James Caverlee from Texas University also researched how terrorist utilizes Twitter as a perfect medium to get funding and attract new members (Alff, Kaghazgaran and Caverlee, 2018). They also compiled many *tweets* that had a connection with ISIS's proselytizing effort, based on their research called *Measuring the Impact of ISIS Social Media Strategy* (Alff, Kaghazgaran, and Caverlee, 2018). It is shown in the table below:

Table 1. Number of ISIS's Twitter Account

Dataset	Accounts	Tweets
ISIS-Tweets	23,880	17,434,323
ISIS-Retweets	551,869	10,436,603
ISIS-Mentions	745,721	19,570,380
Legit-Tweets	23,880	17,454,068
Legit-Retweets	1,753,195	12,175,619
Legit-Mentions	2,161,106	17,479,990

(Source: Alff, Kaghazgaran and Caverlee, 2018)

The existence of young generations (millennials) and their interest in social media have advantages for most terrorist groups like ISIS. Cyber terrorist activism is no longer on how to disable and cripple government information systems. Moreover, it focuses on obtaining their necessities, such as funding and gaining new members. According to *A New Age of Terrorist Recruitment: Target Perceptions of the Islamic State's Dabiq Magazine*, terrorist groups like ISIS tend to recruit young members ranging from 18 to 25 years old (Otterbacher, 2016). Kaylee Otterbacher argued that most of ISIS's new members are still twenty-five (Otterbacher, 2016). She also explained that ISIS is starting to recruit members with higher education and people from middle-class income. Otterbacher

claimed in her research that people from 18 to 25 years old are adaptive to modern technology, and most of them are middle-class people. Many of them are still in the phase of searching for their identity. Hence, they are vulnerable and easy to be manipulated by terrorist groups (Otterbacher, 2016).

Proselytizing also has a severe impact on Indonesia. Terrorist groups use two types of influence to affect and sway Indonesian. The first one is *official propaganda*. They disseminate their ideology by establishing an official website or account on several social media (Putri, 2019). Through its social media account, terrorist groups like ISIS persuade people to join their cause, become regular members, or support them (Putri, 2019). Another way is *unofficial propaganda*. It is a method where a terrorist's ideology spreads through its sympathizer (Putri, 2019). Though it is not direct propaganda, this method is also devastating (Putri, 2019). Social media platforms like Facebook or Twitter emerge as a perfect spreader to disseminate radical ideology (Putri, 2019). Eventually, the information can reach a bigger audience and gain influence (Putri, 2019). Facebook, Twitter, and Youtube are the most effective social media platforms as a radicalized instrument (Lubis, 2017). Three of them have a significant impact on proselytizing people (Lubis, 2017). It can be shown in the table below:

Table 2. Social Media Used as Cyber Radicalization Instrument

Social Media	Method, Purpose, and Function
Facebook	• Multiple accounts • Private messaging and group • Closed group
Youtube	• Media dissemination • Validation • Messaging
Twitter	• Wide broadcast • Multiple accounts • Direct messaging

Source: (Lubis, 2017)

How do security studies see this phenomenon? The author argues that cyber-terrorism is a real threat. With the concept of proselytizing, technology can be used as leverage to inject and spread fear among the people. In addition to using technology, it gives terrorist groups another advantage. There is a higher possibility for them to gain more funding and new members (Kiras in Bayliss et al. 2014). Cavelty (2014) stated that terrorism has a devastating impact on modern

society. The author highlights that the referent object in the context of proselytizing is society itself. Hence, the threat comes from the societal sector. A terrorist group needs new members to sustain their struggle and regenerate members (Bloom, 2017). The advantage of technology has provided them with the opportunity to reach a wider audience. Social media is a platform where terrorist groups can affect people, especially the younger generation, to join their so-called "revolution" (Bieda & Halawi, 2015; Giantas & Stergiou, 2018). Ranging from 18 to 25 years old, these people are vulnerable due to their unstable psychology and inability to counter terrorist ideology (Otterbacher, 2016). Social media's platform is easy to be made as a tool for cyber-terrorism, especially in proselytizing, because it affects and changes human psychology (Otterbacher, 2016; Weimann, 2005). Playing with mutual identity, common religion, and raging hatred towards western culture is useful for terrorist groups to recruit new members from the middle-class economy (Bloom, 2017; Otterbacher, 2016; Weimann, 2005).

Anticipating cyber-terrorism from the context of proselyting surely needs government efforts. Society is the referent object, and people from the middle-class economy are the most vulnerable. States can start filtering social media accounts that have any affiliation with the terrorist groups. Nonetheless, social media is a perfect medium to disseminate violent radical ideology to recruit new members. The information on social media is massive and can influence a wider audience. The government needs to spend its security budget to filter and anticipate the cyber-terrorism threat, impacting their society (Ranggasari, 2019; Tumber, 2019). Besides, the state might want to invest in its information system and its human resources. States can develop a constructive and holistic program by making legal frameworks and combining all fields, including defense, information systems, and even education (Zerzri, 2017). The outcome of this legal framework is a national strategic plan for countering any threat from terrorists. Implementing such kind of program can build awareness, especially to counter any extremization efforts. The cyber-terrorism threat can only be contained if the government acts holistically. Integrating every national aspect from state to private institutions can be an effective way to counter proselytizing.

Coordination and Security

The result of modern technology was the birth of the internet, allowing becoming anonymous. The purpose of anonymity is to ensure the user's privacy when going online or when it comes to communicating with each other via the internet. Unfortunately, this privilege has been misused by a terrorist group from all around the world. Al-Qaeda and ISIS exploit this privilege for their teaching to be spread and gained support from sympathizers. In his research, Stephen Idahosa, *International Terrorism: The Influence of Social Media in Perspective*, examined that Al-Qaeda was the first terrorist group who employed the internet to coordinate its operations (Idahosa, 2017). Al-Qaeda successfully coordinated with its sleeper cells in silence. Almost undetected, the aftermath of the September 11th tragedy was devastating and shocked the whole world. To prepare for such an attack, Al-Qaeda trained and developed its agents to make a bomb and explode it towards the enemy (Idahosa, 2017). They developed a Global Islamic Media Front website to coordinate with their agents, equip them with the skill to make a bomb, and disseminate radical ideology to gain support from the Muslim countries (Idahosa, 2017). In the end, their purpose was to destabilize western countries and spread terror in the heart of society (Idahosa, 2017).

The internet provides not only anonymity but also has an advantage like encryption technology. In the dawn of the internet, encryption was firstly created to protect electronic mail from being tapped by a third party. Indeed, the first objective of encryption was to protect people's privacy when communicating in cyberspace. Nevertheless, encryption can be a threat if the state does not recognize the threat it might possess. Terrorist groups are aware of encryption's capability and see that it may be a gateway to cover their track. When it comes to coordination, it is almost impossible for the authority to track them. As Luke Bertram said, technology had changed the way people were communicating (Bertram, 2016). The flow of communication would be far more comfortable and more straightforward. Unfortunately, privilege is often misused by unwanted groups to do evil deeds. For example, encryption has made the terrorist communication system more secure and hard to detect. It also makes them agile in coordinating with each other.

Cyberspace can indeed be a source of threat to destabilize political stability from the perspective of security studies. As the main actor of International Relations studies, states are responsible for protecting national security and their people's safety, so this threat needs to be appropriately addressed. People cannot put aside the fact that Al-Qaeda and even ISIS have utilized this technology to achieve their primary purpose. The internet and its cyberspace are borderless territories. It is hard to explain where the main boundaries of states in the cyber-world are. There are only a few regulations that conduct law and legal aspects to govern those issues. For example, the Indonesian government should make sure its cyber domain is safe from cyber-terrorism. The government can employ counter intelligence to monitor every anomalous activity to prevent any harmful incidents. The author quoted Idahosa's research that the terrorist group uses social media and cyberspace to coordinate with their agents worldwide (Idahosa, 2017). The counterintelligence system might penetrate and disrupt any communication in cyberspace that involves any terrorist activities.

States cannot ignore the danger the encryption technology has since it protects people's communication inside an email or even daily chatting application. The developers built it to protect the message from being tapped by the third party. Many developing states can decrypt any suspicious information or even put back door systems in the application so the government can monitor terrorist activity in the cyber-world. Unfortunately, if the state does not develop a legal framework to monitor communication in the cyber-world, it can lead to privacy rights violations. In 2014, the US government branch called the National Security Agency was sued because they intentionally tapped world internet communication without any legal framework (Cohn dan Gullo, 2019). Developing legal frameworks may drive them to build strategic corporations between the state, private sector, non-governmental organizations, and individuals. This case could be a perfect benchmarking for Indonesia to be reconsidered. For example, the Indonesian government can cooperate with internet company giants like Google or Facebook to build and establish strategic collaboration to monitor and minimize cyber-terrorism

threats on the cyber-world (Bodin et al., 2015). The first weakness to realize is that the cyber-world is an invisible arena. Therefore to decrease cyber-terrorism activities, the most logical way to do this is to collaborate with actors who know the place. Huge internet companies like Google, Microsoft, or Facebook may be perfect partners. The second one, the cyber-world, is full of anonymity. Many internet giants can uncover anonymity. With the right legal frameworks, the Indonesian government needs to cooperate without jeopardizing people's privacy. Indonesia once worked with Telegram by implementing an information-sharing agreement to detect any terrorist movement. This cooperation can be extended into a holistic agreement with other tech-companies.

Mobility

Technological outreach is borderless. People in a different region can communicate and interact with others in a whole different hemisphere. When a terrorist group can exploit this leverage well, there is no telling of what kind of terror they might do. Kiras said that technology had allowed terrorist groups to mobilize their group in the entire world (Kiras in Bayliss et al., 2014). What will happen if states cannot prevent a threat from terrorist's mobility? Hypothetically speaking, terrorist groups can mobilize and maximize their movement in the global realm. The author has mentioned above that technological outreach does not know any border. To prevent their movement, state actors must collaborate and cooperate (Hough, 2008). Suppose one terrorist group can maximize technology outreach. They can order their hidden agents to terrorize society in a single click of an email or text via social media chat groups.

Even in the context of cyber-terrorism, states are still the main actor in the world politics constellation. They are bound to protect their interest and are driven by it, an inseparable consequence of the state's existence. Cyber-terrorism can affect not only a single region but a whole global realm. Once the government can prevent the threat of proselytizing, coordination, and security, they have to detect their mobility and activity. To mobilize their hidden agent, a terrorist group often move from one country to another. This kind of threat is highly possible to deter by implementing strategic cooperation with other states. The Indonesian government can establish sharing

intelligence mechanisms bilaterally or involving regional organizations (Ramadhan, 2017). Any forms of terrorism, both physical and cyber-terrorism acts, are a threat to a state's political stability. Buzan said that if the threat becomes urgent, it must be institutionalized (Buzan, 1998). Terrorism is a threat to any country in the world, including Indonesia. Hence, implementing sharing intelligence mechanisms is an important thing to do if states want to overcome cyber-terrorism threats.

Many states prefer establishing bilateral or multilateral cooperation. The United States and the British government have collaborated, deterring the threat of cyber-terrorism. Both countries established CERT (Computer Emergency Response Team) cooperation. They work together to identify, monitor, and respond to computer incidents or anomalies in cyberspace to prevent the threat from occurring (Dogrul, Aslan & Celik, 2011). They also developed a legal and working framework to mitigate cyber-terrorist threats and detect their movement in a cyber-world that can disrupt their national security. They also conduct intelligence sharing if they find any peculiar movements and mobilities in cyberspace (Dogrul, Aslan & Celik, 2011). Bilateral cooperation can be implemented not only by developed countries but also by developing countries or vice versa. The Indonesian government indeed can develop robust international cooperation for combating the mobility of the terrorist group. One of them is enhancing cooperation between state and state governments within the Southeast Asia region (Nadjib & Cangara, 2017). Another option is the Indonesian government can support and regulate CERT cooperation within ASEAN members since most of them already have their CERT community (Nadjib & Cangara, 2017).

Harnessing intelligence sharing can be implemented not only on the bilateral level but also on the multilateral level. As mentioned before, if the threat becomes urgent, it must be institutionalized (Buzan, 1998). By utilizing an international organization's role, Indonesia can address this cyber threat with other members. Ranging from regional into a global organization – international institution- can reduce common threats like cyber-terrorism (Ramadhan, 2017). Hence, international organizations can be a hub for the state to share, cooperate,

and prevent the hazardous effect of cyber-terrorism. On the other side, it also provides state information to detect and stop any terrorist mobility from cyberspace. For example, the European Union made a regulation to push its member to share any information that contained terrorist groups (Bodin, Echilley & Quinard-Thibault, 2015). This kind of cooperation among the EU members is significant since they have a common framework and oblige. As a supranational organization, the European Union believes that every cyber-terrorist problem can be adequately addressed due to their common interest. Even though this method is not one hundred percent free from the problem, the EU members know how to counter it. On the other side, Indonesia was involved in the European Union of Cybercrime Prevention (Nadjib & Cangara, 2017). This experience should be a starting point for this government to establish a joint agreement at the ASEAN level for combating cyberterrorism.

CONCLUSION

In this modern era, preventing cyber-terrorism is dependent on the sophistication of technology. Terrorist activity in cyberspace cripples the state's information systems, builds masses, recruits members, and coordinates their operations. To overcome the threat of cyber-terrorism from the context of proselytizing, the Indonesian government needs to develop a holistic approach within its domestic system. State also should build a critical awareness of its citizens; hence they will use technology wisely and filter false information. In the context of coordination, security, and mobility, the government can prevent those threats from other states by implementing bilateral or multilateral cooperation. Indonesia can even build relations with other related institutions. Building legal frameworks is Indonesia's main priority to conduct a robust strategy, such as terrorism-related intelligence data or stopping terrorist cross-border mobility. Cyber-terrorism is not solely one nation's problem, but it is a world's problem. Hence, states cannot ignore the sacredness of cooperation.

REFERENCES

Alff, Majid., Kaghazgaran, Parisa., Caverlee, James. (2018). *Measuring the Impact of ISIS Social Media Strategy*. Available at http://snap.stanford.edu/mis2/files/MIS2_paper_23.pdf. [Accessed, May 7th, 2019]

Aronso, D. Jonathan. (2005). Causes and consequences of the communication and Internet Revolution in John Baylis & Steve Smith (ed), *The Globalization of World Politics: An Introduction to International Relations*. London: Oxford University Press

Bambang, Aa & Fitriana, Idealisa. (2017). Cyberterrorism: Suatu Tantangan Komunikasi Asimetris Bagi Ketahanan Nasional in *Inter Komunika Vol 2 (1), 1-15*.

Bertram, Luke. (2016). Terrorism, the Internet and the Social Media Advantage: Exploring How Terrorist Organizations Exploit Aspects of the Internet, Social Media and How These Same Platforms Could be Used to Counter-Violent Extremism in *Journal for Deradicalization (7)*. ISSN: 2352-9849

Bieda, David & Halawi, Leila. (2015). Cyberspace: A Venue for Terrorism. *Issues in Information Systems Volume 16, Issue III*: Embry-Riddle Aeronautical University.

Bloom, Mia. (2017). Constructing Expertise: Terrorist Recruitment and "Talent Spotting" in the PIRA, Al Qaeda, and ISIS. *Studies in Conflict & Terrorism, 40:7, 603-623*. DOI: 10.1080/1057610X.2016.1237219

Bodin, Silvia., Echilley, Marc., & Quinard-Thibault, Odile. (2015). *International cooperation in the face of cyber-terrorism: current responses and future issues*. Available at http://www.ejtn.eu/Documents/THEMIS%202015/Written_Paper_France_1.pdf. [Accessed, May 10th, 2019]

Buzan, Barry. (1991). New Patterns of Global Security in The Twentieth First Century. *International Affairs* Vol. 67 (3): Wiley-Blackwell

Buzan, Barry et al. (1998). *Security: A New Framework of Analysis*. Colorado: Lynne Rienner

Cavelty, Myriam Dunn. (2014). Cyber Threats in Victor Mauer & Myriam Dunn Cavelty (ed), *The Routledge Handbook of Security Studies*. New York: Routledge

Cohn, Cindy & Gullo, Karen. (2019). *Government Fights to Trap EFF's NSA Spying Case in Catch-22*. Available at https://www.eff.org/deeplinks/2019/04/government-fights-trap-effs-nsa-spying-case-catch-22. [Accessed, May 9th, 2019]

Dogrul, Murat., Aslan, Adil & Celik, Eyyup. (2011). *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber-terrorism*. Available at https://ccdcoe.org/uploads/2018/10/DevelopingAnInternationalCooperation-Dogrul-Aslan-Celik.pdf. [Accessed, May 10th, 2019]

Federal Times. (2016). *Hacker charged with cyber-terrorism gets 20 years*. Available at https://www.federaltimes.com/2016/09/23/hacker-charged-with-cyber-terrorism-gets-20-years/. [Accessed, November 25th, 2019]

Giantas, D & Stergiou, D. (2018). From Terrorism to Cyber-Terrorism: The Case of ISIS. *SSRN Electronic Journal*. DOI:10.2139/ssrn.3135927

Gilsinan, Kathy. (2018). *If Terrorists Launch a Major Cyberattack, We Won't See It Coming*. Available at https://www.theatlantic.com/international/archive/2018/11/terrorist-cyberattack-midterm-elections/574504/. [Accessed, April 10th, 2019]

Gross, M., Canetti, D. & Vashdi, D. (2017). Cyberterrorism: Its Effect on Psychological Well-Being, Public Confidence, and Political Attitudes in *Journal of Cyber Security No 3 (1)*. DOI: 10.1093/cybsec/tyw018

Hough, Peter. (2008). *Understanding Global Security, 2nd Edition*. London: Routledge Taylor and Francis Group.

Idahosa, Stephen. (2017). International Terrorism: The Influence of Social Media in Perspective in the *Journal of Multidisciplinary Research and Development No. 3 [10]*. e-ISSN: 2454-6615

ID-CERT. (2013). CATATAN Tahunan Insiden Siber 2013. Available at http://www.cert.or.id/index-berita/id/berita/41/. [Accessed, January 3rd, 2019].

Kshetri, Nir. (2014). *Cybersecurity and International Relations: The US Engagement with China and Russia*. Accessed from Prosiding FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, Argentina, July 23-25.

Kiras, James D. (2014). Terrorism and Globalization in John Bayliss et al. (ed), *The Globalization of World Politics: An Introduction to International Relations 3rd Edition*. London: Oxford University Press

Lubis, Rizky Reza. (2017). Indonesia's Netizen Potential on Counter-Cyber Radicalization in *Journal of Defense & State Defense, Vol 7 (2), 19-35*.

Nadjib, Muhammad & Cangara, Hafid. (2017). Cyber Terrorism Handling in Indonesia in *The Business and Management Review, Vol 9 (2), 274-283.*

Nye, Joseph S. (2011). *The Future of Power*. USA: Perseus Book Group

Otterbacher, Kaylee. (2016). A New Age of Terrorist Recruitment: Target Perceptions of the Islamic State's Dabiq Magazine in *UW-L Journal for Undergraduate Research*

Pricewaterhouse Cooper. (2014). *Managing Cyber Risk With Insurance*

Press, Gil. (2018). *60 Cybersecurity Predictions For 2019*. Available at https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/#48cf0bc94352. [Accessed, April 10th, 2019]

Putri, Santi Dwi. (2019). Cyber Terrorism: Strategi Propaganda dan Rekrutmen ISIS di Internet Dan Dampaknya Bagi Indonesia Tahun 2014-2019 in *Journal of International Relations Vol 5(4), 827-833*.

Ramadhan, Iqbal. (2017). Peran Institusi Internasional dalam Penanggulangan Ancaman Cyber dalam *Jurnal Populis Vol 2 (4) 2017*. ISSN: 2640-4208

Ranggasari, Ririe. (2019). Banks Invest in Cyber Security. Available at https://en.tempo.co/read/1194168/banks-invest-on-cyber-security. [Accessed, May 8th, 2019]

Rogers, Paul in Paul Williams. (2004). Terrorism in *Security Studies: An Introduction*. USA: Routledge

Samuel, Kuboye Oluwafemi & Osman, Wan Rozaini Sheik. (2014). Cyber-terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences, and Panacea in *JCSMC, Vol. 3, Issue. 5.*

Sarinastiti, Eska Nia & Vardhani, Nabila Kusuma. (2018). Internet dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism Melalui New Media in *Jurnal Gama Societa Vol 1 (1), 40-52.*

Tumber, Rajinder. (2019). *3 Compelling Reasons To Invest In Cyber Security – Conclusion*. Available at https://www.forbes.com/sites/

rajindertumber/2019/01/26/3-compelling-reasons-to-invest-in-cyber-security-conclusion/#76a9d30a6dee. [Accessed, May 8th, 2019]

Ward, Antonia. (2018). *ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa*. Available at https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html. [Accessed, May 7th, 2019]

Weimann, Gabriel. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism, 28:2*

Zerzri, Mayssa. (2017). The Threat of Cyber-terrorism and Recommendations for Countermeasures in the *Center for Applied Policy Research*.