JH Ius Quia Iustum

Volume 29 Issue 1, Januari 2022: pp. 1-23 Copyright © 2022 Jurnal Hukum Ius Quia Iustum Faculty of Law, Universitas Islam Indonesia. ISSN 0854-8498 I e-ISSN: 2527-502X.
Open access at: http://jurnal.uii.ac.id/indek.php/IUSTUM

The Evolution Of Cyberterrorism: Perspectives And Progress From The European Union And Association of Southeast Asian Nation

Haekal Al Asyari
Fakultas Hukum Universitas Gadjah Mada Yogyakarta Indonesia
Jln. Sosio Yustisia Bulaksumur No. 1 Yogyakarta 55281 Indonesia
haekal.al.asyari@ugm.ac.id

Received: 2 Maret 2021; *Accepted*: 31 Agustus 2021; *Published*: 31 Januari 2022
DOI: 10.20885/iustum.vol29.iss1.art1

Abstract

Terrorism, which has caused casualties, economic chaos, and even environmental damage, remains a challenge that must be overcome by the state, whether at the national or international levels. It is crystal clear from the initial circumstances that there is no agreed term to define terrorism, while a new terrorism movement has emerged. By infiltrating cyberspace and hacking critical infrastructure systems, cyberterrorism has generated a shared concern and a collective response by the international community. This article examines these recent developments, from the perspective of the two most progressive regional communities; European Union (EU) and Association of Southeast Asian Nations (ASEAN). With no comparative aim, the author shall try to suggest that although there are different approaches and legal frameworks shared by the two organizations, there is a common goal that is desired to counter cyberterrorism. This paper concludes that the approaches taken by the EU and ASEAN have the similar foundation of value in different ways. The EU places more emphasis on harmonization of national regulations that are supported by regulatory frameworks such as mutual legal assistance. Meanwhile, ASEAN prioritizes diplomatic coordination to increase the capacity and resources of member countries through the e-ASEAN process.

Key Words: Cyberterrorism; European Union; Association of Southeast Asian Nation

Abstrak

Terorisme yang telah menimbulkan korban jiwa, kekacauan ekonomi, bahkan kerusakan lingkungan, masih menjadi tantangan yang harus dihadapi oleh negara, baik di tingkat nasional maupun internasional. Tantangan tersebut terlihat jelas dari fakta awal bahwasanya belum ada kesepakatan dalam mendefinisikan terorisme, sedangkan pergerakan baru terorisme telah muncul. Dengan cara menyusup ke dunia maya dan meretas sistem infrastruktur penting, cyberterrorism telah menimbulkan keprihatinan bersama dan tanggapan kolektif oleh komunitas internasional. Artikel ini akan mengkaji perkembangan tersebut, dari sudut pandang dua komunitas regional yang paling progresif; European Union (EU) dan Association of Southeast Asian Nation (ASEAN). Dengan tujuan yang tidak didasarkan untuk melakukan sebuah perbandingan, penulis akan mencoba menggagas bahwa meskipun terdapat pendekatan dan kerangka hukum yang berbeda yang dimiliki oleh kedua buah organisasi tersebut, terdapatnya tujuan bersama yang diinginkan untuk mengatasi cyberterrorism. Tulisan ini menyimpulkan bahwasanya pendekatan yang diambil oleh EU dan ASEAN memiliki landasan nilai yang sama dengan cara yang berbeda. EU lebih menekankan kepada harmonisasi peraturan nasional yang di dukung oleh kerangka pengaturan seperti mutual legal assistance. Sedangkan ASEAN lebih memprioritaskan koordinasi yang bersifat diplomatis untuk meningkatkan kapasitas dan sumber daya negara anggota melalui proses e-ASEAN.

Kata kata Kunci: Cyberterrorism; European Union; Association of Southeast Asian Nation

Introduction

A patient died at a German Hospital in September 2020 during an attempt to transfer her to another hospital because of a disabled computer system by hackers.[1] While two decades prior, a Missourian wheelchaired man directed Massachusetts schoolchildren to child pornography and posted threats to the school's principal.[2] These two cases goes to show the rapid development and link between cyberterrorism and transnational crime. The prior as an act which utilizes the cyberspace for the commission of terror, while the later has its effects outside of the perpetrator's territory.

Coupling the positive spirit that 'evolution' terminologically has with the controversies of 'terror' might be an understatement. But, as objective as any other researches, it is a part of the academic freedom to inquire the understanding of such dispute in order to formulate the solution. The existence of terror induced acts has started early ever since the medieval times against the Roman Empire, Hindu Thugs, and Christian crusaders between 48 AD until 1956 AD.[3] Some form of terrorism has characterized civilization for the last two thousand years.[4]

It is always believed that cyberterrorism, much like the conventional form will consistently post significant challenges to society.[5] There are various aspects in which cyberterrorism occur that poses different challenges from case to case. Combating such complexity requires a sophisticated form of regulatory framework. From the traditional command-and control regulation enforced by the government, as well as connected and supportive harmonization of laws. Substantially, the law is required to keep up with socio-technological developments that requires additional effort to asses and revise from time to time. Different actions to these approaches can be observed from both national and international levels.

---

[1] J Tidy, "Police Launch Homicide Inquiry after German Hospital Hack", BBC, 18th September 2020, available on https://www.bbc.com/news/technology-54204356, accessed on 28th June 2021

[2] Francis Richardson, "Cyberterrorist Must Serve Year in Jail," Boston Herald, June 6, 2001, accessed on 28th June 2021

[3] M. Bloom, *Dying to Kill: the Allure of suicide terror*, Columbia University Press, New York, 2005, p. 36

[4] Todd Sandler, Daniel G Arce, *Transnational Terrorism*, School of Economic, Cambridge University Press, 2008, p. 1

[5] Bert-Jaap Koops, "Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research", in Babak Akhgar, Ber Brewster, *Combatting Cybercrime and Cyberterrorism: challenges, trends, and priorities,* Springer, Switzerland, 2016, p. 4

European Countries, within the regional context, initially considered terrorism having an internal character that results in the exclusive competence of each state.[6] In the backbone of the Treaty on the Functioning of the European Union (TFEU),[7] minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime of cross-border nature is established.[8] This results in Directive No.2013/40/EU[9] that aims at improving cooperation between the competent authorities of the member states against threat of cyberterrorism.

Travelling down south, ASEAN have held regional forums,[10] cooperation,[11] and declaration in an effort to collectively fight against cybercrime.[12] Despite of its form, altogether these efforts merely go to the extent of harmonizing laws and encouraging the development of national plans of actions in addressing cyber terrorism. From these two glances, it can be identified that both regional approaches lie on the same concept; trying to regulate a transnational phenomenon from the frontiers of national laws.

Problems Formulation

1. How are the different perspectives and progress of legal framework for governing cyberterrorism by the European Union and Association of Southeast Asian Nation?
2. To what extent does the efforts in both regions try to regulate cyberterrorism?

Research Objectives

This paper aims to analyze the similarities over any differences that the EU and ASEAN may have in terms of their regional cooperation to address the issue cyberterrorism. As both regional models having its own unique historical and fundamental basis, but in the realm of cybercrime and cyberterrorism, it is still highly

[6] Izabela Oleksiewicz, "A Legal Assessment of Management of the European Union Cyberterrorism Policy", *Modern Mangement Review*, Vol.22, No.24/3, 2017, pp. 141-152

[7] Article 83, Consolidated Version of the Treaty on European Union [hereinafter "TFEU"], OJ C115/13, 2008

[8] Oleksiewicz *Loc. Cit*.

[9] Directive of the European Parliament and of the Council 2013/40/EU of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA (JOL EU L 218 of 14 August 2013), in Oleksieqiwcz, *Op.Cit.*, p. 146

[10] ASEAN Cyber Security Summit, Singapore, 17th August 2018

[11] ASEAN Leaders' Statement on Cybersecurity Cooperation, 2018

[12] ASEAN Declaration to Prevent and Combat Cybercrime, 2017

influenced by domestic laws and national jurisdiction. It is argued that despite the transnational nature and borderless characteristic of cyberterrorism, both the EU and ASEAN legal frameworks trusts their member states to tackle the issue domestically.

Methodology

This research applies juridical normative method, which mainly analyzes relevant legal instruments and literature with regard to the research problem. This paper primarily assesses international law, the national law of relevant states, as well as literatures relating to cyberspace and terrorism. The analysis is elaborated through a qualitative method on how the EU and ASEAN legal framework progresses in terms of addressing the issue of cyberterrorism.

Result and Discussion

The development of international law has excelled in both regional and national legal frameworks. It is inevitable to unhinge international law from domestic law which makes up the different regional arrangement such as a union, association, or an organization. Put in the context of international issues, various interplays or legal arrangements takes place for the sake of ensuring international legal order. The issue in this paper deals with cyberterrorism. With two questions at hand; the first enquire on how such interplay of regional cooperation progress and views the phenomenon of terrorist in the cyberspace, while the second seeks to understand the progress that has been made so far in trying to regulate cyberterrorism in Europe and Southeast Asia.

Cyberterrorism, in order to accommodate the first enquiry, is taken back to its conventional root as a politically motivated and premeditated act to cause terror. This then transcends borders and with the aid of globalization, transformed into its transnational variant. Information Technology (IT) then creates a new field for such acts, with evermore borderless nature; the cyberspace. This space is then converged with terrorism, inventing a new term 'cyberterrorism'. Despite of its form and place, the goal of such heinous act remains the same, while the regulatory approach requires an extensive inter-state cooperation.

Both the EU and ASEAN, in regards with the second question, seem to have an undisputed common goal for protecting their critical infrastructures in the

cyberspace. This is achieved with optimistic harmonization and mutual recognition of individual state members. While the EU main legal framework is led by regulations and directives, ASEAN strives through agreements and declarations. A major challenge is found in both regions. The EU is hindered by the unsettling efforts at harmonizing criminal law of its member states. While ASEAN is diverged by the "digital divide" among the southeast Asian nations.

Defining Cyberterrorism: Computer and Internet in the Context of Terrorism

Providing a definition as a general rule will contribute towards understanding the context of the problem. There are several formulations converging the term 'cyberterrorism'. Conway argued that it is the combination of 'Cybercrime' and terrorism'[13], while Barry Collin used a more technical term for the prior component with 'Cybernetics'.[14] With both having the component of 'cyber', it is concluded that on a broader scope, the term cyber will solely refer to the concept of 'Cyberspace'.[15] Thus, depicting the act of terrorism that is conducted in, or through, the cyberspace.

Cyberterrorism can refer to unlawful acts, attacks, and threats against computers, networks and the information stored therein (particularly critical infrastructures), with the aim of causing fear and coercion to someone for political (or social) motives which results in violence against persons or property.[16] In this sense, the use of computers could be analogized with a weapon that is used to undermine the society or the government's infrastructures. Within a stricter

[13] M. Conway, "Cyberterrorism: The Story So Far", 2003, http://doras.dcu.ie/496/ 1/info warfare 2 2 2003.pdf, in Nina Olesen, European Public-Private Partnerships on Cybersecurity – An Instrument to Support the Fight Against Cybercrime and Terrorism, Akhgar *Op. Cit.* p. 259

[14] Akhgar *Op. Cit.,* p. 260

[15] For the purpose of this context, Cyberspace means a global borderless domain within the information environment consisting of layered interdependent network of technology infrastructures (including the internet, telecommunications, networks, computer systems, and embedded processors and controllers) that could transmit, receive, store, process, and delete such information, enabled by institutional intermediation and organization, and characterized by decentralization and interplay among the actors, constituencies, and interests.[15] In a simpler sense, Cyberspace is a space characterized by the people, process and technology elements, bounded by logical territories inhabited by zeroes (00000) and ones (11111), *See* Lessig Lawrence, *Code,* Basic Books, New York, (2006), the United States Department of Defence Dictionary of Military and Associated Terms 2010, Joint Publication 1-02, by Office of the Joint Chiefs of Staff, p.83, accessed on 1st of March 2021, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf., Russian-American Cybersecurity Summit, Helsinki, July 16 2018, Choucri Nazli, Co-Evolution of Cyberspace and International Relations: new challenges for the social sciences, World Social Science Forum (WSSF), Montreal, Canada, 2003 https://www.cybersecurityintelligence. com/blog/the-difference-between-Cyberspace-and-the-internet-2412.html accessed on 1st of March 2020, U.M. Mbanaso and E.S. Dandaura, 'The Cyberspace: redefining a new world', *IOSR Journal of Computer Engineering*, Vol. 17, No. 3, 2015

[16] Akhgar *Loc. Cit.*

governmental context, cyberterrorism is a premeditated attack that utilizes the interconnected networks (internet) to cause harm or shut down critical national infrastructure in order to achieve a certain political goal.[17]

Having its transnational nature, territorial and geographical limitation does not limit the battlefield for terror attacks. The emergence of new dimension and a common heritage for mankind,[18] the Cyberspace is also utilized by terrorist groups to launch their attacks and create fear in the society. It is then important to first note that while some actions (or attacks) might constitute a crime, not all of them are induced with terror.[19] Cyber criminals intend to benefit from financial gains as a primary motive, while cyber terrorist aims for a political insurgence.[20] A very common example for the prior is whereby hackers breach data of a certain company in order to sell information illegally to third parties.[21] While the later ranges from innocent trivial protests of patriotism,[22] up to a mass-scale propaganda and violence. For example, several groups of pro ISIS hackers have been active in hacking web hosts to deface internet sites, spreading religious extremist propaganda and open calls for cyberwarfare on social media,[23] as well as in harming online services and businesses.[24] In Malaysia, an ISIS-related hacker group, called "AnonGhost", hacked the Facebook and Twitter accounts of the Royal Malaysian Police (RMP) by changing the profile photo and cover image.[25] In addition, The Cyber

---

[17] US Department of Justice, FBI Law Enforcement Bulletin: Cyber Terrorism, http:// leb.fbi.gov/2011/november/leb-november-2011, accessed on 1st of March 2021

[18] Haekal Al Asyari, "The Cyberspace as a Common Heritage of Mankind: governing jurisdictional limitations of the internet by virtue of international law", *Master Degree Thesis*, University of Debrecen, 2020, *See* Martin C. Libicki C, *Conquest in Cyberspace: national security and information warfare,* Cambridge University Press, United Kingdom, 2007, De Bruno De Padirac, *The International Dimensions of Cyberspace Law,* Routledge, 2003, Jason Whittaker, *The Cyberspace Handbook,* Routledge, London, 2004, Kriangsak Kittichaisaree, "Public International Law of Cyberspace"*, Law, Governance and Technology Series*, Vol.32, Springer, Switzerland, 2017

[19] United Nations Manual on the Prevention and Control of Computer-Related Crime, International Review of Criminal Policy, No.43 and 44, New York, 1994, p. 4

[20] Conway *Loc. Cit* . p. 6.

[21] Malaysian Airlines website 'compromised' by hackers, https://www.bbc.com/news/world-asia-30978299, accessed on 22nd July 2021, Tokopedia data breach exposes vulnerability of personal data, https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html, accessed on 22nd July 2021

[22] Malaysia sites hacked after blunder over Indonesian flag, https://www.bbc.com/news/world-asia-40996126, accessed on 22nd July 2021

[23] Dominika Giantas, Dimitrios Stergiou, "From Terrorism to Cyber-Terrorism: the case of ISIS", SSRN: https://ssrn.com/abstract=3135927, Accessed on 1st of March 2021

[24] Sociedade Portugesa de Inovacao (SPI), "Overview of Cybersecurity Status in ASEAN and the EU", Ref. Ares(2018)5582066 - 31/10/2018

[25] PDRM's Facebook, Twitter accounts hacked, https://www.malaymail.com/news/malaysia/2015/07/13/pdrms-facebook-account-hacked/932533, Accessed on 1st of March 2021

Caliphate hacking group managed to hack the Malaysia Airlines website in January 2015 causing the website to become inaccessible[26]

Transnational terrorism is not the only subject exclusive to trends. Cyberterrorism also went through two stages of burgeon. The first deals with the infrastructure and layers of the internet where such act of terror is induced. While as a consequence of the first, the second surrounds the changes in society on how crime and terrorism have occurred.[27] There are two main problems that are posed by the threat of cyberterrorism. According to Keiran Hardy and George Williams, the first deals with existing terrorist groups, such as Al-Qaeda will use computer technology to disrupts and cause chaos against critical national infrastructure. The second is the menace of 'hacktivists' to attack websites and other 'non-essential' infrastructure for political motives to which potentially amount to a serious threat that is equal to the first problem.[28] The later however is argued that disrupting the website of a government institution or a corporation for whatever political motives will not amount to the severity that conventional terrorism have exhibited.[29] Nevertheless, both instances are deserved to be raised as a national concern by national legislators. Governments both in the western and eastern part of the world have enacted a wide range of laws directed specifically towards the threat of terrorism, but very little have specifically constructed a framework that compromises the role of computer and technology within the act of terror.

Cyberterrorism: Where it started, how it has progressed, and Where it is now

It is important to conceptualize the 'beginning' and the 'present' that is implied in this section as the start of (conventional) terrorism that transformed into its transnational variety, which then took its latest (but not final) form in the cyberspace. Thus, it is only right to begin with at least one definition of what terrorism is. As a criminal act intended or calculated to provoke a state of terror in the general public, by either individuals or a group of persons for political

[26] Malaysia Airlines website hacked by 'Cyber Caliphate', https://edition.cnn.com/2015/01/25/asia/malaysia-airlines-website-hacked/index.html, Accessed on 1st of March 2021

[27] Koops, *Op. Cit.,* p. 5

[28] Keiran Hardy, George Williams, "'What is Cyberterrorsim'? Computer and Internet Technology in Legal Definitions of Terrorism", in Thomas M. Chen, Lee Jarvis, Stuart Macdonald, *Cyberterrorism: understanding, assessment, and response*, Springer, London, 2014, p. 2,

[29] Conway M, "Hackers as terrorist? Why it doesn't compute", *Comput Fraud Secur*, No. 12, 2003, pp. 10-13

purposes in any unjustifiable circumstances unjustifiable, with whatever political, philosophical, ideological, racial, ethnic, religious, or other nature that may be invoked to justify them.[30] While the collective or group version of such actions is believed to be a collection of individuals belonging to a non-state entity that rely partially or exclusively[31] on terrorism to achieve its objectives.[32]

When a premeditated threat, or actual use of violence to attain a political goal through fear, coercion, or intimidation, and its ramifications transcend national boundaries through the nationality of the perpetrators and/or human or institutional victims, location of the incident, or mechanics of its resolution it is claimed to be as an act of Transnational Terrorism.[33] During the modern era of transnational terrorism, terrorists crossed borders and, in some instances, staged incidents in foreign capitals to focus world attention on their cause or grievance.[34]

Terrorists have shared ideologies since the start of the modern era of transnational terrorism in 1968 – the leftists sought to overthrow capitalist governments, while the fundamentalists have followed a fatwa issued against the "enemies" of Islam. These common ideologies and calls to action motivated terrorists to strike in concert against target countries. Some political events have simultaneously resulted in attacks in many countries.[35] For example, a spate of terrorist attacks followed the Arab-Israeli conflicts, the US retaliatory raid against Libya in April 1986, the Gulf War in January 1991, and the Abu Ghraib prison revelations in April 2004.

---

[30] United Nations General Assembly Resolution 51/210, Measures to Eliminate International Terrorism, 17 December 1996; A/RES/49/60 9 December 2006; Security Council Resolution 1566, 8 October 2004.

[31] Leonald Weinberg, Ami Pedazhur, and Sivan Hirsch-Hoefler, *The Challenges of Conceptualizing Terrorism, Terrorism and Political Violence*, Routledge, UK London, 2004, pp. 477-794.

[32] For the history of contemporary terrorism, four years stand out as turning points: 1968, 1979, 1983, and 2001. In 1968, Latin American insurgents launched their so-called urban guerrilla strategy, and Palestinians initiated the tactic of terrorism as publicity stunt, which soon evolved into serious violence. As we have seen, both undertook terrorist type activities as a substitute for the guerrilla warfare that neither was competent to wage *See* Seth G. Jones and Martin C. Libicki, *How Terrorist Groups End: Lessons for Countering Al Qa'id*, RAND, Washington, DC, 2008, p. 7

[33] Sandler *Loc. Cit.*

[34] *Ibid*

[35] Gaibulloev Khusrav, Sandler Todd, and Sul Donggyu, "Common Drivers of Transnational Terrorism: Principal Component Analysis", Forthcoming Economic Inquiry, *Western Economic Association International,* Vol.51(1) 2013, pp. 707-721

Terrorist in the globalized order today crosses borders and stage incidents in foreign capital to focus world attention on their cause or grievances.[36] Thus what can be understood by the term transnational terrorism. Whilst Terrorism is the premeditated use or threat to use violence by individuals or subnational groups against non-combatants in order to obtain a political or social objective through the intimidation of a large-scale audience beyond that of the immediate victim. Two key words that must be highlighted from the definition is violence and political or social motive. Without violence or its threat, terrorists cannot induce a political decision maker to respond to their demands. Terrorist broaden their audience beyond the immediate victim by making every attack appear to be random, making everyone feeling at risk. Unlike ordinary criminal acts, terrorist incidents are well planned and often well-executed attacks, where the risks, costs, and payoffs carefully.[37]

Recent trends have shown that new dimensions of terror and its global nature is born out of the wombs of globalization, giving birth to new magnitude such as;[38] increment of religiously motivated terrorism, geographical shift from Europe and Latin America to Northern Africa, the Middle East, South Asia and Southeast Asia, rise of international/transnational terrorism, inseparability of internal and external security of states as potential targets, new networks of organized crimes, growth of non-state actors' involvement, hybrid terrorist-criminal groups.

Perspectives and Progresses in the EU and ASEAN

The advancement of cyberspace influences the practice of terrorism by providing new means and field for its action. Instead of turning against individuals or destroying physical property, cyberterrorists cause destruction and disruption in cyberspace.[39] Conducting attacks in the cyberspace does not require abundant financial or human resources making it an attractive option for terrorists. There are two possibilities of how cyberterrorism is conducted. The first is combined with the conventional, and physical terrorist attacks; by ways of

[36] *Ibid.*

[37] *Ibid.*

[38] Daljit Singh, "The Terrorist Threat in Southeast Asia" in: ISEAS (Ed.), Southeast Asia 2003-2004, Regional Outlook.

[39] Dorothy E Denning, "A View of Cyberterrorism Five Years Later", *Calhoun: the NPS Institutional,* https://calhoun.nps.edu/bitstream/handle/10945/37160/Cyberterror_2006.pdf?sequence=1, Accessed on 1st of March 2021

disabling or disrupting emergency services during a certain operation (telecommunication, power plants, air traffic controls, financial networks). While the second leans towards the premeditated aspect of conventional terrorism, dealing with plans or propaganda and raising financial funds.[40] The section below will not specifically address any of the two instances, but rather combine both aspects to fit in the aforementioned description of cyberterrorism.

Peace and security are an inevitable agenda within the four freedom of the European Union without internal frontiers. On a worldwide scale, after the series of events of September 11, European terrorist groups still remain significantly active, but more focus has been shifted on for Europe as a logistics base for terrorist groups.[41] This triggered a logical counter terrorism action plans by the EU such as pushing forward legislative proposals in order to harmonize national laws in the realm of internal security.[42] Subsequent to the Madrid bombings,[43] the EU evolved it's peculiar perspective to focus on prevention, through the identification of the underlying factors that can lead to terrorism, or the so-called 'root causes' of terrorism.[44] Following the London bombings,[45] the EU have mirrored the UK approach by adopting the prevent, protect, pursue, and respond strategy.[46] This design institutionalizes the intra-European collaboration in counterterrorism.

The term cyberterrorism, in Europe, first appeared in Sweden where reports showed that there were computer threats aimed at the destruction of information and technology system, or known as one of the critical infrastructures.[47] The EU

---

[40] Mitko Bogdanoski, Drage Petreski, "Cyber Terrorism – Global Security Threat", *International Scientific Defence, Security and Peace Journal,* 327.88:004.738.5-027.22, p. 60

[41] Frank Gregory, "The EU's response to 9/11: a case study of institutional roles and policy processes with special reference to issues of accountability and human rights*"*, *Terrorism and Political Violence*, 17:1-2, 1050123, DOI: 10.1080/09546550590520618, 2005

[42] Rik Coolset, "EU Counterterrorism Strategy: value added or chimera?", *Royal Institute of International Affairs*, Vol. 86, No. 4, 2010, pp. 857-873

[43] Madrid Bombings of commuter trains in Spain killing 191 and wounding 1,800 people https://edition.cnn.com/2013/11/04/world/europe/spain-train-bombings-fast-facts/index.html, accessed on 18th of December 2019

[44] Soolse*t Loc. Cit.*

[45] 7 July 2005 London Bombings, the series of coordinated Islamist terrorist suicide attacks in London, England, that targeted commuters travelling on the city's public transport system during the morning rush hour https://www.britannica.com/event/London-bombings-of-2005

[46] CONTEST, *The United Kingdom's Strategy for Countering Terrorism*, Secretary of State for the Home Department by Command of Her Majesty, 2018

[47] Oleksiewicz *Op. Cit.* p. 141

Framework decision on combating terrorism, a feature that stands out prominently is the material element of terrorist offences, the potential infrastructure that could be the target of terrorist attacks includes; extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or a private property likely to endanger human life or result in major economic loss.[48] The framework covers a wide range of critical infrastructures that could be undermined by terror attacks in the cyberspace based on the different sectoral arrangement.[49] Such cross-sectoral approach which the EU have taken ensures the coverage of critical infrastructure where domestic laws will act as a *lex specialis.* A double layer of legal framework and regulatory body delegates the enforcement and judiciary against cyber related attacks in the EU states.

It can be said that European states still focuses their fight against terrorism from within national borders. One of the efforts is by harmonizing and providing a general standard for legal systems to deem any illegal access or interference to the computer system as a crime.[50] This effort is however subject to the never-ending debate of EU policy harmonization of criminal law within the regional cooperation.[51] The sector of organized crime could be considered as a core dilemma for the effort to harmonize criminal law legislation within the EU. There are three main international legislation that deals with tackling the issue of organized crime. The first is Joint Action on making it a criminal offence to participate in a criminal organization in the Member States of the European Union. Second is 2000 United Nations Convention against Transnational Organized Crime. Third is the Council Framework Decision on the Fight against Organized Crime (2008).

---

[48] EU Framework Decision of 13 June 2002 on Combating Terrorism (2002/475/JHA), Art. 1

[49] United Nations Office of Counter-Terrorism, "The Protection of Critical Infrastructure Against Terrorist Attacks: compendium of good practices", 2018

[50] Directive of the European Parliament and of the Council 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA(JOL EU L 218 of 14 August 2013.), Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (JOL EU L, No. 69, of 16 March 2005.).

[51] Fransesco Calderoni, *Organized Crime Legislation in the European Union, Harmonization and Approximation of Criminal Law, National Legislations and the EU Framework Decisions, on the Fight Against Organized Crime*, Springer, Heidelberg, 2010, p. 21

The aspect of sovereignty lies as the core fundamentals of EU Criminal Law. It is one of the only part[52] of the glorified harmonization where the capacity to impose power to pool sovereignties become less.[53] Because of the impact of criminalization and punishment from individual and European societies, criminal law is negotiated at the national level in order to produce a parameter of the relationship between the individual and state.[54] This however does not eliminate the resistance to the transfer of power from the individual state to the Union level, particularly in the context of adopting uniform criminal law. This creates both opportunities and challenges for crimes that have evolved and transcends national borders; particularly with terrorism that occurs in the cyberspace. Nevertheless, national criminal justice systems in the European Union are expected to interact under the EU instruments on the basis of mutual trust and maximum automaticity.[55] These bases are essential when considering the factor of territoriality; to which determines jurisdiction among the nation states. The concept of borderless area goes beyond the economic and political realm. Security and justice (particularly under the third pillar) are the spear end of conceptualizing criminal law in the EU.[56]

The European Commission adopted a provision to categorize any attack through interference with information systems to be punishable as terrorist attacks in any of its member states. Through its directives and relying on mutual recognition, along with the European Investigation Order[57], it enables prompt international cooperation for investigating and resolving cyber related terrorist attacks.

South-eastern countries did not deem terrorism an urgent security concern prior to September 11.[58] Before the Bali bombing of 2012, terrorism was not seen

---

[52] The discourse of company law is also highly debatable among EU nations, *See* Dirk Van Gerven, Paul Storm, *The European Company,* Vol II, Cambridge University Press, Cambridge, 2008

[53] Valsamis Mitsilegas, *EU Criminal Law*, Hart Publishing, Portland, 2009, p. 321

[54] *Ibid*

[55] *Ibid.,* p. 322

[56] This results in significant development of criminal law principles. Democracy, transparency, and legitimacy appears prominently when mutually recognizing the State's criminal law. At the end of it, the enforcement of criminal law in the EU aims to protect fundamental rights of its citizens.

[57] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

[58] Senia *Loc. Cit.*

as a significant threat to the nation where most part belonging to the Indonesian media generally reinforcing a stance of denial.[59] It can be observed that cooperation for counter-terrorism in ASEAN can be divided into two: political and reinforcement. With the prior, there are levels of national and multilateral declarations made in the interest of such political intent. In 2001, the Declaration on Joint Action to Counter Terrorism emphasized the urgency of combating terrorism in a comprehensive manner.[60] So forth agreements between Philippines with Indonesia and Malaysia as a three-way anti-terrorist pact.[61] Multilaterally, mechanisms are constructed in the ASEAN Ministerial Meeting on Transnational Crime where it emphasizes capacity building and intelligence procurement.[62] Dialogue partners of the ASEAN includes the joint declaration made with the United states[63] and China.[64]

A novelty from the temporary threat of terrorism in Southeast Asia is that it operates operationally and ideologically linked, rooted from fractions of oppressed communities.[65] A cursed blessing of nations that are rich in culture and indigenous communities, living and adapting to the never-ending wave of globalization. Hence, the agendas of such terrorist groups do not only cover national, but also regional and global spheres causing legal and political providing challenges for nations to cooperate and integrate to certain extents of policy making.

ASEAN, in the context of cyberterrorism and other forms of transnational crimes, agrees that such phenomenon falls under common security concern. Despite the birth of ASEAN coming from an economic womb, such security concerns inarguably revolve around economic issues. Therefore, in the last

---

[59] Leonard C. Sebastian, "The ASEAN Response to Terrorism", UNISCI Discussion Papers, Institute Defence and Strategic Studies, *Network of Scientific Journals from Latin America*, the Carribean, Spain and Portugal, 2003

[60] ASEAN Declaration on Joint Action to Counter Terrorism, Brunei 5th of November 2001

[61] The agreement was planned to be made as alongside the 31st ASEAN Summit in Philippines

[62] Most recent meeting (13th) was held in Bangkok, 26-28 November 2019

[63] ASEAN-United States of America Joint Declaration for Cooperation to Combat International Terrorism, Bandar Seri Begawan, 1st of August 2002

[64] Joint Declaration of ASEAN and China on Cooperation in the Field of Non-Traditional Security Issues, 6th ASEAN-China Summit, Phnom Penh, 4th of November 2002

[65] Rohan Gunaratna, "ASEAN's Greatest Counter-Terrorism Challenge: The Shift from "Need to Know" to Smart to Share," in Christian Echle, Rohan Gunaratna, Patrick Rueppel, and Megha Sarmah, (Eds.), *Combatting Violent Extremism and Terrorism in Asia and Europe: From Cooperation to Collaboration*, Konrad-Adenauer-Stiftung and S. Rajaratnam School of International Studies, Stifung, Singapore, 2018

decade, a set of security issues has expanded the ASEAN cooperation and legal framework.[66]

A unique feature to Southeast Asian region that is worth mentioning is the presence of "digital divide". Particularly in terms of infrastructure development and economic disparities, along with socio-political capacity which amounts to significant challenge in adjusting both the domestic legal framework and enforcement of ASEAN countries. Hence, an understanding of the differences is essential to determine the collective regional response towards cyberterrorism.

Responses and Efforts from the EU and ASEAN

Similar to any other domino effect that was caused by the events of September 11, the EU instrument and legal framework also sought to prioritize terrorism as an international agenda. The EU "war on terrorism" applied many anti-organized crime measures and introduced legislation and intense restriction of civil liberties.[67] In the EU substantive criminal law, the Treaty on the Functioning of the European Union (TEFU)[68] enables approximation for defining the offences of organized crime including terrorism. Back in 2010, the United Kingdom's national security strategy lists cyber-attacks by terrorist as one of the highest priority risks.[69] In terms of criminal procedure, the TFEU enables adoption of minimum rules in the fields of mutual admissibility of evidence, rights of individuals in criminal procedure, rights of victims of crime[70] and other specific areas unanimously deliberated in a Council Decision.[71]

The EU has put a range of catalogue of legal, practical, and support tools to underpin a European region of internal security under the Treaty of Lisbon that reinforces the legal framework to pool efforts and ensure peace, liberty, and

---

[66] Nicholas Thomas, "Cyber Security in East Asia: Governing Anarchy", *Asian Security*, Vol.5 No.1, 2009, pp. 3-23,

[67] Orlova AV, Moore JW, "Umbrellas" or "Building Blocks?": defining international terrorism and transnational organized crime in international law", *Houston Journal of International Law*, Vol.27 2005, pp.265-310, *See* Calderoni p. 35

[68] Consolidated version of the Treaty on the Functioning of the European Union (TFEU), 2012/C 326/01, 2012

[69] Cabinet Office, "The National Security Strategy: a strong Britain in an age of uncertainty", Cm 7953, 2010

[70] TFEU Article 82 Para 2

[71] Calderoni *Op. Cit.,* p. 12

security in the region.[72] Contrary to the South-eastern approach, the EU tends to see the war on terror from a much broader context where addressing issues such as poverty, health, and education, as well as migration is deemed necessary as an essential complimentary program for the rule of law and good governance.[73]

EU counterterrorism strategy has a similar yet more complex scheme to the US model due to the intricate institutional structure of the Union and by differences of threat perception as well as the various cultural and political traditions within the region.[74] Counter-terrorism has always been a theme within the EU policies which was central to the security cooperation between EC Member States. Originally set out in the European Political Cooperation and became a regular high-level congregation, counter-terrorist policies were created as a result of domestic terrorism in several EC countries.[75] However, the inception of anti-terrorism policies into the third pillar hierarchy somehow vanished amongst other internal security concerns such as illegal immigration and organized crime.[76] It is not until the last decade the the EU gave emphasis to international/transnational terrorism, where credit goes to Islamic fundamental terrorism.[77]

The adoption of the European Arrest Warrant serves as a legal instrument in which it facilitates extradition proceedings based on the principle of mutual recognition and acts as a cornerstone for criminal justice cooperation.[78] The warrant approves 32 types of offences with detailed procedural rules based on the system of mutual recognition, obliging member states to acknowledge others' judicial decisions, therefore replacing the common extradition procedures.[79]

One of the fundamental bases of EU's commitment against terrorism can be seen in the security agenda which sets out principles for EU to respond effectively

---

[72] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, the European Agenda on Security, COM 185, Strasbourg, 2015

[73] Tamara Makarenko, *Europe Adapts to new Terrorist Threats,* JIR, 2003, pp. 24-27

[74] Coolset, *Op. Cit.,* pp. 858

[75] Anderson, *et.al.*, *Policing the European Union. Theory, Law, and Practice,* Clarendon Press, Oxford, 1995

[76] Monica Den Boer, "9/11 and The Europeanisation of Anti-Terrorism Policy: A Critical Assessment", Policy Papers No.6, Groupement d'études et de recherches, 2003

[77] *Ibid., Anderson Et al*

[78] 2002/584/JHA, Council Framework Decision of June 13th on the European Arrest Warrant and the Surrender Procedure between Member States, 2002

[79]Monica *Loc. Cit*

to security threats primarily terrorism and radicalization where Europol is the center for it.[80] In 2001, the Europol expanded its mandate to establish a Task Force for the Fight against terrorism[81] where its principal task is to provide operational support to Member States in investigations following terrorist attacks. Additionally, EUROPOL also had a basis of an Interim Information System, in the form of Counter Terrorism Support system designed to store sensitive terrorist related activities.[82]

The one source of binding instrument that is belonging to ASEAN, is its Convention on Counter Terrorism created in 2007.[83] It aims to strengthen regional counter-terrorism efforts with special highlights covering not only regional definitions of 'terrorist offences' but also international ones.[84] Unfortunately, along with the nature of the organization, some of the articles contained are garnished with broadly drafted baseline of legal and political consensus, such as the guarantees on the right of fair treatment.[85] The strong emphasis on national legal frameworks of the member states is somehow becoming a wider challenge in terms of strengthening regional cooperation when it comes to considering terrorism as a domestic matter.[86]

One major note of the ASEAN framework is that policy-making in the region is firmly adhered by the so-called "ASEAN Way'.[87] Where such principal becomes a double-sided knife for having a consensus based in respect to each other's national sovereignty and non-interference in domestic matters which produces a

---

[80] *Ibid*

[81] EUROPOL Counter Terrorism Centre (ECTC), https://www.europol.europa.eu/newsroom/news/europol%25E209s-european-counter-terrorism-centre-strengthens-eu%25E209s-response-to-terror

[82] Monica *Loc. Cit*

[83] ASEAN Convention on Counter Terrorism, 13 January 2007 (entered into force 27 May 2011)

[84] *Ibid* Article I

[85] *Ibid* Article VII

[86] E4J University Module Series: Counter-Terrorism, Module 5: Regional Counter-Terrorism Approaches, https://www.unodc.org/e4j/en/terrorism/module-5/key-issues/asian-region.html

[87] The "ASEAN Way" refers to a methodology or approach to solving issues that respects the cultural norms of Southeast Asia where policy making constantly utilize compromise, consensus, and consultation in the informal decision-making process it above all prioritizes a consensus-based, non-conflictual way of addressing problems. *See also* Rodolfo C. Severino, "The ASEAN Way and the Rule of Law", at the International Law Conference on ASEAN Legal System and Regional Integration, Kuala Lumpur 3rd of September 2001, https://asean.org/?static_post=the-asean-way-and-the-rule-of-law accessed on 22nd of December 2019

slower and more fragile product of not just legislation, but also ratification, and implementation to keep up with the dynamic threat.[88]

An approach by way of securing cyberspace is present in two forms as an effort to combat cyberterrorism in ASEAN. First is the attempt to improve regional capacity and resources through e-ASEAN process. The second encompasses direct attempts from transnational subversion of national security, particularly those stemming from the activities of criminal and terrorist organization (contrasting to APEC's approach with cyber issues being mainly dealt with under the telecommunications area).[89] In regards to the prior attempt, the e-ASEAN initiative was introduced in the Manila summit in 1999[90] and constructed a broad-based and comprehensive action plan including physical, legal, logistical, social and economic infrastructure needed to promote an ASEAN e-space, as part of an ASEAN positioning and branding strategy. The later takes from in framework agreements and cooperation that expands to the Telecommunications and IT ministers (TELMIN) which triggered several multilateral and bilateral mutual recognition agreements.[91] Consequently, such efforts created a closer progress for cooperation in addressing cyber related issues such as cybercrime and cyberterrorism.

The beginning of the pinnacle for ASEAN's response is the establishment of the ASEAN Regional Mechanism to Combat Cyberterrorism which produced the ARF Cyber Terrorism summit and opened doors for information—sharing amongst ASEAN member states. [92] Four years later, the ASEAN Police Chiefs (ASEANAPOL) was established as a program for members of regional police forces to be trained in cybercrimes by Interpol. Such concrete effort is facilitated by linking the regional crime database and cooperating with Interpol's I-24/7 Global Police Communication System of wanted criminals.[93] These efforts suggest that concrete actions by ASEAN states have been taken to the extent of not only

---

[88] Marguerite Borelli, "ASEAN Counter-terrorism weaknesses: Analysis", *Eurasia Review* https://www.eurasiareview.com/16102017-asean-counter-terrorism-weaknesses-analysis/, accessed on 22nd of December 2019, Rohan *Loc. Cit.*

[89] Thomas *Op. Cit.,* p. 11

[90] ASEAN Declaration on Transnational Crime Manila, 20 December 1997

[91] *Ibid*

[92] Co-Chairs Summary Report ARF Cybercrime Capacity-Building Conference Bandar Seri Begawan, Brunei Darussalam April 27-28, 2010

[93] Reports on the APEC Technomart III, as contained in: Rodney Chester, "Crooks tipped to ride cyber crime wave," The Courier Mail, November 2, 1999

harmonizing the different laws, but also in legal and institutional forces in order to combat cyberterrorism.

Conclusion

First, there are many factors that contribute to the occurrence of cyberterrorism. The challenge does not only come from the fact that it will always develop along with technology, but the double threat that it poses from the nature of cyberspace having a borderless element, and terrorism having a transnational effect. Therefore, each region has a different spontaneous response in combatting cyberterrorism. Generally, both EU and ASEAN have tried to create a regulatory framework to accommodate the eradication of terrorism in the cyberspace. Specifically, for the EU, states in Europe are bound under the TFEU. This acts as a gateway in harmonizing counter-terrorism laws under the conception of criminal law. On the other hand, South-eastern countries are dictated by the ASEAN way. Thus, a far-less degree of harmonization efforts are made within each countries legal system. Both these differences has their own consequences presented in the following conclusion.

Second, EU wise, the topic of counter-terrorism in regional policy making is not yet on the highest extent or harmonization. Nation states are still reluctant and rather conservative on the internationalization of their criminal justice system, as it is considered as the last line of national sovereignty.[94] As a result, a hybrid system of policy-making process is made with somehow a federalized structure of criminal justice co-operation. One of the challenges that Europe still has to face is with regards to harmonizing laws (particularly criminal) of the member state. While in ASEAN, agreements and declarations have been made, but it is only up to the safest extent, recognizing the unique 'way' that ASEAN adopts in respecting sovereignty of its members. The issue with ASEAN is the existence of a 'digital divide' that poses more challenges than opportunities that requires the legal framework to depend on economic, political, and indefinitely technological developments of the different nations.

Conclusively, regional response to the threat of cyberterrorism is generated from the interface between inter-state cooperation on the one hand, and

[94] Monica *Loc. Cit*

interaction within domestic realm on the other. To this very end, the success of regional fight against cyberterrorism will highly depend on the capabilities and will of individual member states to act against terrorist within their own borders.

Bibliography

Book

Akhgar Babak, Brewster Ber, *Combatting Cybercrime and Cyberterrorism: challenges, trends, and priorities,* Springer, Switzerland, 2016

Anderson, *et.al*., *Policing the European Union. Theory, Law, and Practice,* Oxford, Clarendon Press, 1995

Bloom, M, *Dying to Kill: the Allure of suicide terror*, Columbia University Press, New York, 2005

Calderoni, Fransesco, *Organized Crime Legislation in the European Union, Harmonization and Approximation of Criminal Law*, National Legislations and the EU Framework Decisions, on the Fight Against Organized Crime, Springer, Heidelberg, 2010

Chen Thomas, M., Jarvis Lee, Macdonald Stuart, *Cyberterrorism: understanding, assessment, and response*, Springer, London, 2014

Echle, Christian, Gunaratna Rohan, Rueppel Patrick, and Sarmah Meghan , (Eds.), *Combatting Violent Extremism and Terrorism in Asia and Europe: From Cooperation to Collaboration*, Konrad-Adenauer-Stiftung and S. Rajaratnam School of International Studies, Stifung, Singapore, 2018

Jones, Seth G. and Martin C. Libicki, *How Terrorist Groups End: Lessons for Countering Al Qa'id*, RAND, Washington, DC, 2008

Lawrence, Lessig, *Code,* Basic Books, New York, 2006

Libicki, C Martin, *Conquest in Cyberspace: national security and information warfare,* Cambridge University Press, United Kingdom, 2007

Mitsilegas, Valsamis, *EU Criminal Law*, Hart Publishing, Portland, 2009

Padirac, De Bruno *The International Dimensions of Cyberspace Law,* Routledge, 2003

Sandler Todd, Arce G Daniel, *Transnational Terrorism*, School of Economic, Cambridge University Press, Cambridge, 2008

Van Gerven, Van Dirk, Storm Paul, *The European Company,* Vol II, Cambridge University Press, 2008

Weinberg, Leonard, Pedazhur Ami, and Hirsch-Hoefler Sivan, *The Challenges of Conceptualizing Terrorism, Terrorism and Political Violence*, Routledge, UK London, 2004

Whittaker, Jason, *The Cyberspace Handbook,* Routledge, London, 2004

Journal

Conway, M, "Hackers as terrorist? Why it doesn't compute", *Comput Fraud Secur*, No. 12, 2003

Daljit Singh, "The Terrorist Threat in Southeast Asia" in: *ISEAS (Ed.)*, Southeast Asia 2003-2004, Regional Outlook

Frank Gregory, "The EU's response to 9/11: a case study of institutional roles and policy processes with special reference to issues of accountability and human rights", *Terrorism and Political Violence*, Vol.17 No.1-2, 2005

Gaibulloev, Khusrav, Sandler Todd, and Sul Donggyu, "Common Drivers of Transnational Terrorism: Principal Component Analysis", Forthcoming Economic Inquiry, *Western Economic Association International,* Vol.51(1) 2013

Oleksiewicz, Izabela, "A Legal Assessment of Management of the European Union Cyberterrorism Policy", *Modern Mangement Review*, Vol.22 No.24/3, 2017

Kittichaisaree, Kriangsak, *Public International Law of Cyberspace,* Law, Governance and Technology Series, Springer, Switzerland, Vol. 32, 2017

Sebastian, Leonard C., "The ASEAN Response to Terrorism", UNISCI Discussion Papers, Institute Defence and Strategic Studies, *Network of Scientific Journals from Latin America*, the Carribean, Spain and Portugal, 2003

Bogdanoski, Mitko, Drage Petreski, "Cyber Terrorism – Global Security Threat", *International Scientific Defence, Security and Peace Journal,* 327.88:004.738.5-027.22, 2013

Monica Den Boer, "9/11 and The Europeanisation of Anti-Terrorism Policy: A Critical Assessment", Policy Papers No.6, *Groupement d'études et de recherches*, 2003

Thomas, Nicholas, "Cyber Security in East Asia: Governing Anarchy", *Asian Security*, Vol.5 No.1, 2009

V, Orlova A, Moore JW,"Umbrellas" or "Building Blocks?": defining international terrorism and transnational organized crime in international law", *Houston Journal of International Law*, Vol.27 2005

Rik Coolset, "EU Counterterrorism Strategy: value added or chimera?" *Royal Institute of International Affairs*, Vol. 86, No. 4, 2010

Makarenko, Tamara, "Europe Adapts to new Terrorist Threats," JIR, 2003

Mbanaso, U.M. and E.S. Dandaura, 'The Cyberspace: redefining a new world', *IOSR Journal of Computer Engineering*, Vol.17 (3), 2015

Treaties

ASEAN Convention on Counter Terrorism, 13 January 2007

Consolidated Version of the Treaty on European Union, OJ C115/13, 2008

Other Legal Documents

ASEAN Cyber Security Summit, Singapore, 17th August 2018

ASEAN Declaration on Joint Action to Counter Terrorism, Brunei 5th of November 2001

ASEAN Declaration on Transnational Crime Manila, 20 December 1997

ASEAN Declaration to Prevent and Combat Cybercrime, 2017

ASEAN Leaders' Statement on Cybersecurity Cooperation, 2018

ASEAN-United States of America Joint Declaration for Cooperation to Combat International Terrorism, Bandar Seri Begawan, 1st of August 2002

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, the European Agenda on Security, COM 185, Strasbourg, 2015

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (JOL EU L, No. 69, of 16 March 2005.)

Council Framework Decision of June 13th on the European Arrest Warrant and the Surrender Procedure between Member States, 2002

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

Directive of the European Parliament and of the Council 2013/40/EU of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA (JOL EU L 218 of 14 August 2013)

Directive of the European Parliament and of the Council 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (JOL EU L 218 of 14 August 2013)

EU Framework Decision on Combating Terrorism (2002/475/JHA), 2002

Joint Declaration of ASEAN and China on Cooperation in the Field of Non-Traditional Security Issues, 6th ASEAN-China Summit, Phnom Penh, 4th of November 2002

United Nations General Assembly Resolution 51/210, Measures to Eliminate International Terrorism, 17 December 1996

Internet

Dominika Giantas, Dimitrios Stergiou, "From Terrorism to Cyber-Terrorism: the case of ISIS", SSRN: https://ssrn.com/abstract=3135927, Accessed on 1st of March 2021

Dorothy E Denning, "A View of Cyberterrorism Five Years Later", *Calhoun: the NPS Institutional,* https://calhoun.nps.edu/bitstream/handle/10945/37160/Cyberterror_2006.pdf?sequence=1, Accessed on 1st of March 2021

E4J University Module Series: Counter-Terrorism, Module 5: Regional Counter-Terrorism Approaches, https://www.unodc.org/e4j/en/terrorism/module-5/key-issues/asian-region.html

EUROPOL Counter Terrorism Centre (ECTC), https://www.europol.europa.eu/newsroom/news/europol%25E209s-european-counter-terrorism-centre-strengthens-eu%25E209s-response-to-terror

https://www.malaymail.com/news/malaysia/2015/07/13/pdrms-facebook-account-hacked/932533, Accessed on 1st of March 2021

https://edition.cnn.com/2013/11/04/world/europe/spain-train-bombings-fast-facts/index.html, accessed on 18th of December 2019, Accessed on 1st of March 2021

Malaysia Airlines website hacked by 'Cyber Caliphate', https://edition.cnn.com/2015/01/25/asia/malaysia-airlines-website-hacked/index.html, Accessed on 1st of March 2021

Marguerite Borelli, *ASEAN Counter-terrorism weaknesses:* Analysis, Eurasia Review https://www.eurasiareview.com/16102017-asean-counter-terrorism-weaknesses-analysis/, accessed on 22nd of December 2019

Rodolfo C. Severino, *The ASEAN Way and the Rule of Law,* at the International Law Conference on ASEAN Legal System and Regional Integration, Kuala Lumpur 3rd of September 2001, https://asean.org/?static_post=the-asean-way-and-the-rule-of-law Accessed on 1st of March 2021

United States Department of Defense Dictionary of Military and Associated Terms (2010, Joint Publication 1-02, by Office of the Joint Chiefs of Staff, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf., Accessed on 1st of March 2021

US Department of Justice, FBI Law Enforcement Bulletin: Cyber Terrorism, http://leb.fbi.gov/2011/november/leb-november-2011, accessed on 1st of March 2021

World Social Science Forum (WSSF), Montreal, Canada, 2003 https://www.cybersecurityintelligence.com/blog/the-difference-between-Cyberspace-and-the-internet-2412.html accessed on 1st of March 2020,

Miscellaneous

Cabinet Office, The National Security Strategy: a strong Britain in an age of uncertainty, Cm 7953, 2010

CONTEST, The United Kingdom's Strategy for Countering Terrorism, Secretary of State for the Home Department by Command of Her Majesty, 2018

Ester Herlin-Karnell & Claudio Matera, External dimensions of the EU counter-terrorism policy, Centre for the Law of EU External Relations, CLEER working papers 2014/2

Frank Umbach, *EU-ASEAN Political and Security Dialogue at the Beginning of the 21 Century: prospects for interregional cooperation on international terrorism,* SSOAR Open Access Repository

Haekal Al Asyari, *The Cyberspace as a Common Heritage of Mankind: governing jurisdictional limitations of the internet by virtue of international law*, Master Degree Thesis, University of Debrecen, 2020

Keiran Hardy, George Williams, 'What is Cyberterrorsim'? Computer and Internet Technology in Legal Definitions of Terrorism, 2014

Reports on the APEC Technomart III, as contained in: Rodney Chester, "Crooks tipped to ride cyber crime wave," The Courier Mail, November 2, 1999

Russian-American Cybersecurity Summit, Helsinki, July 16 2018

Sociedade Portugesa de Inovacao (SPI), "Overview of Cybersecurity Status in ASEAN and the EU", Ref. Ares(2018)5582066 - 31/10/2018

United Nations Office of Counter-Terrorism, The Protection of Critical Infrastructure Against Terrorist Attacks: compendium of good practices, 2018