IBIMA Publishing
Journal of Southeast Asian Research
http://ibimapublishing.com/articles/ JSAR /2022/384427/
Vol. 2022 (2022), Article ID 384427, 12 pages, ISSEN: 2166-0832
DOI: 10.5171/2022.384427

Research Article

Jurisdiction Issues in Cyberspace: An Overview in Respect of Brunei and Malaysia Compared to The United States' System

[1]Nehaluddin AHMAD and [2]Norulaziemah ZULKIFFLE

[1]MA, LLB, LLM (Lucknow University, India)
LLM (Strathclyde University, UK), LLD. (Meerut University, India)
Professor of Law, University Islam Sultan Sharif Ali (UNISSA), Brunei Darussalam

[2]LL.B & BSL, LL.M (University Islam Sultan Sharif Ali (UNISSA), Brunei Darussalam

Correspondence should be addressed to: Norulaziemah ZULKIFFLE; aziemah.zulkiffle@gmail.com

Received date:10 February 2022; Accepted date:22 June 2022; Published date: 20 July 2022

Academic Editor: Rehana Parveen

Abstract

Cyberspace is a borderless world. It refuses to accord geopolitical boundaries. This means that cyberspace has no physical boundaries and limitations. Despite the benefits it offers, it places a unique challenge for states mainly on the issue of jurisdiction and sovereignty. This article aims to discuss a comparative study of how the United States, Brunei and Malaysia, tackle the issue of jurisdiction and sovereignty in the borderless world of the Internet. The United States addresses specific requirements such as the minimum contacts test, reasonable anticipations, and the effects that have to be met in dealing with the issue of jurisdiction in cyberspace. However, Brunei and Malaysia have different approaches as compared to these. These countries exercise that the location of the data and the accused at the time of the act are adequate to establish jurisdiction. It finds that the national law of Brunei and Malaysia is still insufficient to protect their cybersecurity compared to the United States which has a wider jurisdiction over the defendant than other states with certain requirements.

Keywords: Sovereignty, Jurisdiction; Internet

Cite this Article as: Nehaluddin AHMAD and Norulaziemah ZULKIFFLE (2022), "Jurisdiction Issues in Cyberspace: An Overview in Respect of Brunei and Malaysia Compared to The United States' System", Journal of Southeast Asian Research, Vol. 2022 (2022), Article ID 384427,
DOI: 10.5171/2022.384427

Introduction

The Internet is often regarded as the most significant invention in human history. (Brockman, J., 2000) It has become a highly convenient instrument for commerce and communication in this modern-day, resulting in the emergence of a virtual world with no physical boundaries and limitations. According to Dareportal 2022, there are 4.9 billion Internet users in the world today, which is equivalent to 58.4 percent of the world's population. Due to the blast growth in Internet usage, the issue of jurisdiction has become a critical issue where many jurisdictional challenges have arisen, (Frinklea, K.M., 2013) placing a unique challenge for regulators of law, especially on the jurisdiction boundaries and sovereignty. (Maier, B., 2018).

The Internet's technological structure and global interconnection provide state and non-state actors with a platform to operate against a wide range of targets without being constrained by geography or territorial boundaries. For instance, states can increasingly exploit the Internet as a fresh way of participating in classic statecraft, such as espionage and low-cost, asymmetric offensive operations. Similarly, non-state actors frequently utilize cyberspace to carry out negative operations that endanger persons, businesses, and nations. ISIS, for example, utilizes the Internet to command and manage its operations, disseminate poisonous propaganda, recruit new members, and instigate worldwide terror. (Corn G.P and Taylor R., 2017)

The Internet's challenge to the traditional concept of jurisdiction is complex but can be narrowed down into two issues. Firstly, the sovereignty of the borderless Internet. The Internet is not owned or controlled by any single company or government; hence it is a borderless area. This means that you are simultaneously everywhere and nowhere when you are online. Perhaps, the most distinguishing feature of this remarkable borderless medium is its ubiquity, where you may travel from one location to another with just a click of a button. For instance, two people could communicate from the opposite poles of the earth. With that being said, geography is a remarkably meaningless idea. (Crews Jr. C.W and Thierer A., 2013) Secondly, the jurisdiction encompasses the state's sovereignty and its ability to act in legislative, executive, and judicial approaches. However, the Internet has no defined border or territory to exercise a jurisdiction which contradicts the traditional concept of jurisdiction described in International Law. (Sachdeva A.M., 2007)

In other words, when applied in the realm of the Internet, the traditional concept of jurisdiction has resulted in overlapping jurisdictions of multiple states. The Internet's borderless nature potentially allows for hundreds of different states to claim jurisdiction over any given act committed within the Internet, which confuses the applicable legal regime in many situations. (Chia C.W, 2018)

Developing countries like Brunei, (B. Marco *et al*, 2018) and Malaysia still lacks Internet laws and IT systems. Their legislation and statutes dealing with the Internet are still insufficient to cope with the evolving Internet crimes.

This article aims to compare the concept of sovereignty and jurisdiction in international law with the borderless world of the Internet. Section III of this article discusses the issue of jurisdiction under international law and how the United States tackles this issue. To compare, Part IV of this article discusses the conflict of jurisdiction in the borderless Internet encounters by Brunei and Malaysia, how these two states tackle such matters and the laws that help regulate the Internet in Brunei and Malaysia. Lastly, it shows that Brunei and Malaysia have different approaches than the United States in dealing with the issue of sovereignty and jurisdiction

in the borderless world of the Internet. It finds that the national law of Brunei and Malaysia is insufficient to protect their cybersecurity compared to the United States which has a wider jurisdiction over the defendant from other states subject to the requirement, which will be further discussed.

The Sovereignty Issues and Challenges in Borderless Internet

Throughout the years, many aspects of human life have been affected ever since the expansion and growth of the Internet. States, companies, and individuals have all made great use of the opportunities provided by the Internet. The cyber realm has challenged the conventional political, social, and economic systems of international society. It has dramatically expanded the speed, volume, and range of communications, fundamentally altering how nations are governed. Businesses offer services and public goods, individuals communicate and form social networks on the Internet, and citizens participate in civil society. (Liaropoulos A., 2013)

Nevertheless, whether based on a norm of international law or a concept of international comity, every state must respect the sovereignty of others and must not interfere with how other nations exercise their sovereignty. Territoriality is an evitable outcome of sovereign equality among states and peaceful coexistence. Jurisdiction principles, both personal and prescriptive, were formed from a presumption about the absoluteness of borders and sovereign authority within them and were grounded in political practicality. The traditional rule defines sovereignty as "jurisdiction extends and is restricted to everyone and everything inside the sovereign's territory as well as his people wherever they may be." In other words, "laws extend so far as but no further than the sovereignty of the state which puts them into force.". (Ryder R.D., 2001)

The idea that the sovereign had ultimate power over all people and objects within its geographical boundaries was quite strong, as well as the expansion of international trade which resulted in the escalation of cross-border movement of people, and commission of actions made inevitable the relaxation of this presumption to some extent. (Ryder R.D., 2001) Inarguably, in the physical world, the borders will remain notable so long as the land and everything it contains remains to be viewed as something which can be controlled or owned.

However, this idea does not apply in the world of the Internet. With just over 58% of the global population connected online, it is more difficult for the state to control data flow within and across their sovereign territories. (McDonald N., 2018) Frequent and still ongoing debates of how the borderless world of the Internet challenges the country's sovereignty on how to handle these issues, particularly on cyber-warfare, cyber-security, and cyber sovereignty. (Chen J.D.J., 2015)

China's 'Great Firewall' demonstrates that Internet censorship can coexist with economic growth. (Saakashvili E., 2019) In other words, the world is seeking a method to enjoy the benefits of the Internet while preventing the downside of the Internet. In simple terms, the countries want to be open for business but closed for politics. (Lewis J. and Roth A., 2019)

Currently, states still retain the ability to monitor and regulate Internet activity within and outside their borders. For instance, the capability to ban companies from conducting business within their borders applies to Internet-based companies. This is further illustrated in the case of Netflix and Facebook. Despite having over one billion cross-border users, neither Netflix nor Facebook are welcome or available in China. Similarly, the social media app 'Tik Tok,' where India has outlawed the use of the Chinese social media app 'Tik Tok' has barred Amazon and Walmart from holding inventory. (Economist, 2019)

Jurisdiction issues and challenges in the borderless Internet

It is widely known that the Internet has no geographical boundaries, and hence, is borderless. However, the laws and policies are mostly limited to the territory and the scope of national limitations. The judgment issued by the national courts has no extraterritorial effects on other countries unless under any other specific circumstances. (Velasco C., et. al., 2016) This part will discuss the concept of Jurisdiction under International Law, which creates a significant challenge to the idea of borderless of the Internet and how the United States handles these challenges.

The concept of Jurisdiction under International Law

According to James Crawford, Jurisdiction is "a state's competence under international law to regulate the conduct of natural and jurisdiction persons." In another definition, it is also known as "one of the most obvious forms of the exercise of sovereign power." (Legal Status of Eastern Greenland, Denmark v Norway, 1933)

Hence, it can be understood that the jurisdiction defines the legitimate scope of governmental powers. It covers the right of a state to prescribe, give effect to and adjudicate upon violations of normative standards for regulation of human conduct. In other words, the term jurisdiction encompasses the state's sovereignty and its ability to act in legislative, executive, and judicial approaches. In the legislative concept, a state has the authority to establish rules for regulating the conduct of persons. The authority of the sovereign also has the power to execute its laws and affect the implementation of its laws, which refers to the enforcement jurisdiction. Finally, curial jurisdiction refers to the power of the courts of sovereignty to hear and adjudicate a certain matter in a dispute. (Sachdeva A.M., 2007)

On the other hand, international law is a cornerstone of the modern international order, and its relevance to state and non-state cyber actions has long been recognized. However, due to cyberspace[1] unique and rapidly evolving nature, its ubiquitous interconnectivity, lack of segregation between the private and public sectors, and incompatibility with traditional geographic concepts, there are complex and unresolved questions about how international law applies to this domain.(Corn G.P and Taylor R., 2017) The main question is how and what are the measurements for the states to tackle these issues of sovereignty and jurisdiction. The following part discusses how the United States illustrates how to handle these issues.

The United States' way of handling these challenges

Due to the lack of existing law in addressing the jurisdiction concerning the Internet, the courts in the United States have been obliged to apply classic jurisdictional assessments to cases in this new realm. Traditionally, the jurisdictional requirements have been based on the parties' location and activity to determine which state's law should be applied. (Gray T.L., 2002)

A court does not have authority over every person in the world. Hence, a court must first evaluate whether it has personal jurisdiction over the parties before deciding the case. A plaintiff may not sue a defendant in a foreign jurisdiction unless the defendant has established some relationship with that forum that leads him to reasonably expect to be sued there.

Personal jurisdiction refers to a court's ability to rule over a specific party, in other words, the territorial extent of a court's power over a particular party. The law of personal jurisdiction as it exists now only makes sense if it is considered a series of decisions,

[1] 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.'

beginning with the case of Pennoyer v. Neff, which is interested in territorial limits. (Barnard J.S., 2016)

Following the turn of the century and the nation's mobilization in the 1890s, the Supreme Court reassessed personal jurisdiction and redefined the traditional test (Barnard J.S., 2016) from which the requirements will be further discussed as follows:

i. The Test of Minimum Contacts

A minimum contact can be defined as the connections between a non-resident defendant and the forum state where the action is filed, sufficient to establish competent jurisdiction over that defendant, for instance, conducting business within the state, having a contract with the resident of the state, incorporating in the state and visiting the state. (Cornell, n.d)

The standard of minimum contacts is a significant starting point for jurisdictional analysis of online parties and remains to adapt to the borderless world of the Internet. (Gray T.L., 2002) In the *International Shoe v Washington*, the Supreme Court first made the rule by including the criterion of 'minimum contacts' on the reason that due process only requires that in order to subject a defendant to a 'judgment in personam' (personal jurisdiction); he must have specific minimum contacts with the forum such that 'the maintenance of the suit does not offend traditional notions of fair play and justice.' (International Shoe Co. v Washington, 1945) This means that the present concept is established based on minimum contacts with the state, even if one of the parties is not physically present. In addition, the territorial concept of jurisdiction is still maintained but is given a wider dimension.

However, the minimum contacts test formed based on the jurisdiction in the International Showcase was not a mere mechanical test but depended on the "quality and nature of the activity concerning the fair and orderly administration of laws." (International Shoe Co. v Washington, 1945)

The case of McGee v. International Life Insurance Co. established that minimum contacts can be created by consent, which occurs when a party enters a contract that includes being litigated in the forum. A party who seeks to object to the court's jurisdiction must first sign a clause declaring that they agree on the matter and will respect all laws and rules imposed by the state, otherwise they will lose the right to raise such an obligation. A party must also prove to the court that a party's connections do not amount to the level that would allow the court to exercise jurisdiction. If a party refuses or failed to cooperate with such a request, the Supreme Court has ruled that they have waived their right to object to jurisdiction. (McGee v International Life Insurance Co., 1957)

ii. Reasonable Anticipation

The minimum contacts test was still broad and vague. However, it was strengthened in *Hanson v. Denckla* in 1958. The court held that an action is required 'by which the defendant purposefully avails itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws.' (Hanson v Denckla, 1958) In other words, a court would not have jurisdiction unless it could be proven that the defendant had purposefully availed himself of the privilege of conducting business in the forum. The vital element of foreseeability requires realistic and reasonable anticipation of being hauled into court in the forum state and not just the probability that a product would make its way there. (Cybersell, Inc v Cybersell)

Therefore, the 'purposeful availment test' was revised so as not to be interpreted too literally. It became sufficient that the defendant joined or affiliated himself with the forum in some manner through his acts, invoking or targeting the forum's legislation. The precautions against excessive jurisdiction got increasingly intricate as the scope of jurisdiction grew wider. The Supreme Court held in *World-Wide Volkswagen Corp. v.*

Woodson that, even if minimal contacts exist, the court may decline to exercise personal jurisdiction if doing so would be unreasonable, taking into account factors such as the burden on the defendant, the forum State's interest in adjudicating the disputes, the plaintiff's interest in obtaining convenient and effective relief, and the shared interest of the several States in furthering fund-raising efforts. (World-Wide Volkswagen Corp. v. Woodson, 1980)

However, there is also a significant problem that arises from this requirement. The argument of reasonability in personal jurisdiction often contradicts the exercise of the rule of assumption of jurisdiction based on universal access to online pages. (Sachdeva A.M., 2007)

Hence, the US courts balance these claims in the case of *Zippo Manufacturing Co v Zippo Dot Com* by categorizing all online activities into three categories: Firstly, the active websites; Secondly, websites that allow information to be exchanged with the host computer and passive websites. The response must be straightforward for the first and last categories because "this involves [s] the knowing and repetitive transfer of computer data via the Internet." (Zippo Manufacturing Co v Zippo Dot Com, 1996)

iii. "Effects" cases

The Supreme Court based jurisdiction in the "effects' cases on the principle that if the defendant knew his behavior would harm the plaintiff, he must fairly and reasonably presume to have anticipated being "haled into court where the injury occurred." The "effects" cases are significant in the world of borderless Internet because any action on the Internet often has effects in various jurisdictions.

Therefore, it is evident that this method allows the court to have jurisdiction over the defendant from other states, subject to the requirement as discussed above. This method holds better security to the citizens of the United States in conducting any business through the Internet.

The conflict in borderless Internet in Brunei and Malaysia

The rapid development of the Internet and information technology, particularly in the 1990s, led to governments all over the world, particularly in developed countries, adopting the Internet in their daily lives to improve their quality of service in the business, socializing and communicating with the public, particularly stakeholders and interest groups such as the private sector, mass media, professional groups, and other civil society organizations. The current dynamics of Internet-related public policy have likewise evolved at a quick pace. Brunei Darussalam and Malaysia are not left behind to grab the opportunity the Internet offers. (Bhirowo M., 2018)

Brunei Darussalam

Brunei Darussalam is a constitutional Islamic monarchy state located on the northern coast of the Borneo Island in Southeast Asia. It is a small country with a small population that encompasses a total area of 5,765 square kilometers with over 161 kilometers of coastline along the South China Sea. (Information Department, n.d.)

Brunei's significant challenge in the borderless world of the Internet is the rapid escalation of cybercrime and the rapid growth and expansion of the Internet, citing money laundering, fraud, and the propagation of extremist ideologists. (Bandial A., 2018)

Although Brunei is a small country, it is not spared from encountering cybercrime on the borderless Internet. On 4th May 2010, Brunei's court dealt with its first cybercrime offense, which saw a Filipino national convicted and sentenced. The defendant was charged with hacking into a wireless Internet connection without authorization and using a stolen credit card number to make $2,720 worth of online purchases. The defendant was punishable under Section 6(1)(a) of the Computer Misuse Act and under Section 420 of the Penal Code, where he was found guilty and sentenced to six months' imprisonment

for his first offense and received a further 22.5 month's jail for his illegal credit card misadventure. (E-Governmental National Centre, 2010) By 2018, Brunei has prosecuted 14 cybercrime offenses relating to the Internet, including defamation, spreading false information, and uploading obscene material on social media platforms. (Bandial A., 2018)

Some countries follow a 'technologically neutral approach.' They appear to consider the existing criminal law sufficient to deal with cybercrime or any other wrongdoings done on the Internet. From that perspective, information systems and the Internet may be treated as an instrument of the offense. (Vagias M., 2016)

Other legal systems have enacted legislation to penalize criminal acts done through the Internet. States disagree in identifying minimum contacts with their territory that a form of cyber-criminality should have to enable them to assert territorial jurisdiction. A 'significant nexus with domestic jurisdiction', such as the location of the data or the accused at the time of the act, is adequate to establish jurisdiction under the UK Computer Misuse Act, which is contrary to the approaches made by the United States. Following this, Brunei also considers the offender's location, the impacted computer, or the affected computer system at the material time to be sufficient. (Vagias M., 2016)

The government of Brunei Darussalam has made significant progress in the field of Internet security by implementing several key initiatives, which include implementing Regulations for Computer Abuse in June 2000, which is an order to make provisions to secure computer material from unauthorized access or modification, as well as other related matters. (Bhirowo M., 2018) This order was officially executed as an act in 2007 and known as the Computer Misuse Act. (Computer Misuse Act of Brunei Darussalam, Chapter 194)

IT Protective Security Services (ITPSS) was one of the earliest organizations founded in 2003 to act as a local pioneer in the field of information security solutions, offering penetration testing, digital and mobile forensics, including data recovery, managed security services (MSS), cyber and info-sec awareness training, physical and electronic security and security event management. ITPSS consists of a team of experts in information and cyber security and an experienced management team who are certified with security qualifications.(Bhirowo M., 2018)

Subsequently, ITPSS is also responsible for handling the Brunei Computer Emergency Response Team founded in 2004. It is a Brunei Darussalam referral agency for dealing with Internet threats and computer security problems. BruCERT has actively improved public awareness about cyber security and cyber safety through outreach projects such as student lectures, roadshows, publications, radio shows, newspaper adverts, television commercials, and cinema advertisements. Following that, a Vigilance Program for Internet Ethics and Cyber Security was held. The initiative began holding seminars for students, professors, and parents of students in local educational institutions in 2009. (Bhirowo M., 2018)

Brunei Darussalam was the first country in the region to adopt a Child Online Protection Framework, based on the International Telecommunication Union's (ITU) Child Online Protection Initiative in 2013. Such a framework is required for coordinating the actions of stakeholder agencies to ensure that the necessary safeguards are in place to ensure child safety online when children and young people are increasingly using social media to communicate and are becoming vulnerable to cyberbullying, harassment, and sexual predators. (Sharbawi Z., 2011)

Next, the Development of National Cyber Security Framework called e-Government National Center (EGNC) under the Prime Minister Office (PMO) was also started in 2014. It aims to provide a comprehensive framework for managing cyber security at the national level. (Bhirowo M., 2018) The

National Cyber Security Framework was completed in 2017. The framework establishes minimal and mandatory security standards for risk management and compliance. It also includes Essential Information Infrastructure Protection 7 (CIIP) principles and a standard strategy for correctly and quickly sharing critical information on Cyber Incidents. (Sharbawi Z., 2011)

Concerned about the rise in cyber-attacks, Brunei Darussalam's Autoriti Monetari Darussalam (AMBD) issued ICT Risk Management Guidelines to local banks and finance companies in 2015. The guidelines recommended relevant internationally recognized standards to manage risks associated with technology-based financial systems and practices. (Gan R.Y., 2018)

The procurement of more advanced C4SI equipment as part of the Royal Brunei Armed Forces' continuing modernization would render military infrastructure and assets more vulnerable to cyber-attacks by integrating net-centric weapon and communication systems. As a precaution measure, the Ministry of Defence has designated two (2) units to lead cybersecurity efforts: the Defence Security Branch for policy enforcement and the Defence Information Technology Unit for technical and operational procedures, with a proposal to create a dedicated Cyber Defence Unit to integrate all military cyber security components and standard operating procedures. (Gan R.Y., 2018)

Despite these efforts and initiatives, the laws and IT system are still insufficient to protect and secure cybersecurity in Brunei. It needs more consistency in amending the legislation to suit the present situation. Compared to the United States, it allows better security to its citizens since the jurisdiction is widened by being able to apply jurisdiction over the defendant from other states subject to the requirement discussed before. Therefore, Brunei must evaluate the existing and future vulnerabilities of its technological innovations and analyze its ability to respond to cyber threats that continue to evolve to build a sustainable and credible national cyber defense framework.

Malaysia

Malaysia is located in Southeast Asia. The Federation of Malaysia consists of 13 states. It is divided into 11 states in Peninsular Malaysia, also known as West Malaysia, and two comprise East Malaysia, which is situated on the island of Borneo. Hence, Malaysia is bordered by Thailand in the north, Indonesia in the South, and the Philippines in the east. (Division of Industry and Community Universiti Sains Malaysia, 2013)

As early as 1997, Malaysia has adopted the Computer Crimes Act to combat any criminal acts done through the Internet. Despite the existence of cyber laws, Internet crime remains challenging to combat, and as such, adequate laws are needed to arrest the criminals.

Like Brunei, Malaysia also appears to consider that particular legislation needed to penalize any criminal acts through the Internet. Malaysia considers the location of the offender, the impacted computer, or the affected computer system at the material time to be sufficient. This can be supported by Article 9(2) and Article 9(3) of the Computer Crimes Act 1997, which reads:

"(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time."

"(3) Any proceeding against any person under this section which would be a bar to subsequent proceedings against such person for the same offence if such offence was committed in Malaysia shall be a bar to further proceedings against him under any written law relating to the extradition of persons, in respect of the same offence outside Malaysia."

The Computer Crimes Act of 1997 is utilized in Malaysia to tackle cybercrime. However, this regulation only applies to computer misuse and does not encompass a wide range of computer-related activities. The Digital Signature Act of 1997 sets rules for employing digital signatures to safeguard online transactions, while the Copyright Act of 1997 protects against infringement of copyrights. Acts such as the electronic commerce act of 2006 and the personal data protection law of 2010 govern e-commerce transactions and the processing of personal data.

Several government entities, such as the Malaysian Communications and Multimedia Commissions and the Ministry of Science, Technology, and Innovation (MOSTI), deal with cyber threats (MCMCs). MOSTI is responsible for formulating a framework for ICT policy at the national level. Its objective is to develop policies to protect its essential information infrastructure (CNII). CNII is related to every physical and virtual asset, system, and function significant to the country, and its security is critical. Cyber Security Malaysia (CSM) was established to provide technological security services and preserve NCSP policies. Emergency services, quality management, professional development, strategic engagement, and research are all under CSM's purview. MOSTI is also in charge of the Malaysia Computer Emergency Response Team, which deals with computer emergencies (MyCERT). MCMC, on the other hand, oversees broadcast, Internet service provider (ISP), postal and courier services, as well as the authority over digital certificates. (Singh M.M., Frank R. and Wan Zainon W.M.N, 2021)

One of the strategies used to detect cyber offenders and solve complex cybercrime cases is computer forensic investigation. It is adopted by a computer forensic specialist who examines data from storage media using particular digital forensic tools. The computer forensic investigation team in Malaysia is accessible not only at the Cheras Computer Forensic Laboratory but also at the Cybersecurity Office and the Military Office. The computer forensic expert in Malaysia follows a number of guidelines, which include: (Mohamed D., 2012)

(a) United Nations Manual on Computer Forensic Examination;

(b) IOCE Guidelines for Best Practice in the Forensic Examination of Digital Technology;

(c) NTI Computer Incident Response Guidelines; and

(d) FBI forensic investigations manual.

It can be seen that Brunei and Malaysia have the same system when involved with the Internet and cybersecurity. Brunei and Malaysia are sufficient with the system where the location of the data and the accused at the time of the act are adequate to establish jurisdiction. Hence, these states have no jurisdiction over the defendant where the conduct was done in other states which is contrary to the United States. Similar to Brunei, Malaysia may perhaps consider the system of the United States to be amended in the national law especially in combating cyber threats.

Conclusion

The Internet, as a significant and revolutionary invention in human history, has become a highly convenient instrument for worldwide commerce and advanced communications in this modern era. The steady growth of the Internet has exponentially resulted in the emergence of a virtual world with no physical boundaries and limitations. Despite the benefits that the Internet offers, it creates a hypercritical concern over the states of the world on the issue of jurisdiction and sovereignty.

The concept of the Internet has brought challenges to jurisdiction, which involves two main issues. Firstly, the sovereignty of the borderless Internet, which means the Internet is not owned or controlled by any single company or government. Secondly, the jurisdiction encompasses the sovereignty of the state and its ability to act in legislative, executive and judicial approaches. Yet, the

Internet has no defined border or territory to exercise a jurisdiction which contradicts the concept of jurisdiction as defined in International Law.

Currently, states still retain the ability to monitor and regulate Internet activity within and outside their borders. For instance, the capability to ban companies from conducting business within their borders applies to Internet-based companies. For instance, neither Netflix nor Facebook are welcome or available in China.

In the United States, the court reassessed personal jurisdiction and redefined the traditional test through fulfilling the three requirements: the test of minimum contacts, reasonable anticipation, and "Effects" cases. Subject to these requirements, the court in the United States is allowed to have jurisdiction over the defendant from other states, thus, it holds better security to the citizens of the United States in conducting any business through the Internet.

Brunei Darussalam, however, is not immune from having to encounter cybercrime in the borderless world of the Internet, ranging from citing money laundering, fraud, to the propagation of extremist ideologies. However, Brunei Darussalam has a different approach to handle this issue compared to the United States. Brunei appears to consider that particular legislation is needed to penalize any criminal acts that occur through the Internet, in which Brunei considers the location of the offender, the impacted computer, or the affected computer system at the material time to be sufficient.

This can be proven when the government of Brunei Darussalam has established a number of authorities and laws concerning the Internet by implementing several key initiatives and creating comprehensive frameworks, especially in dealing with the rise of cyber-attacks nowadays.

Similar to Brunei, Malaysia also encounters Cybercrime which triggers its jurisdiction. However, to combat this challenge, Malaysia follows the same approach as Brunei where Malaysia considers particular legislations needed to penalize any criminal acts done through the Internet as laid down in Articles 9(2) and 9(3) of the Computer Crimes Act of Malaysia 1997. In Malaysia, there are also several other legislations and government entities that help to combat this issue. Through these comparisons, it finds that the national law of Brunei and Malaysia is insufficient to protect their cybersecurity compared to the United States which has a wider jurisdiction over the defendant from other states subject to the requirement discussed before. Therefore, it can be suggested that Brunei and Malaysia may follow the footstep of the United States in combating the Internet and cyberspace jurisdiction issues in the nearest future by asserting the requirements discussed in their national law.

References

- B. Marco *et al*, (2018) 'Brunei Cybersecurity Masterplan 2018', S. Rajaratnam School of International Studies 14
- Bandial A., 'AG: Strengthen current laws to address new cyber treats' *The Scoops* (Bandar Seri Begawan, 14 August 2018)
- Barnard J.S., (2016), 'A Brave New Borderless World: Standardization World End Decades of Inconsistency in Determining Proper Personal Jurisdiction in Cyberspace Cases', Seattle University Law Review, 40(249), 254.
- Bhirowo M., (2018), 'Brunei Darussalam's E-Government Strategy in Overcoming Cyber Threats' (2018) 4(3) Jurnal Pertahanan, 4(3), 146.
- Brockman J., (2000) The Greatest Inventions of the Past 2,000 Years, Simon and Schuster, Manhattan, New York.
- Chen J.D.J., (2015), "Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization" *Georgetown Journal of International Affairs* [Online] [Retrieved October 12, 2015], https://www.georgetownjournalofinternationalaffairs.org/online-edition/data-

sovereignty-cybersecurity-and-challenges-for-globalization/
- Chia C.W, (2018), 'Sketching the Margins of a Borderless World: Examining the Relevance of Territoriality for Internet Jurisdiction' Singapore Academy of Law Journal 30, 834.
- Computer Misuse Act of Brunei Darussalam, Chapter 194.
- Copyright Act 1997 of Malaysia.
- Corn G.P and Taylor R., (2017) 'Sovereignty in the Age of Cyber', American Journal of International Law Unbound, 111, 207.
- Cornell, (n.d)., 'Minimum Contacts' *Cornell Law School* [Online], [Retrieved 6 February 2022], https://www.law.cornell.edu/wex/minimum_contacts> accessed on 6th February 2022.
- Crews Jr. C.W and Thierer A., (2003), 'Who Rules the Net', Cato Institute, xv.
- Cybersell, Inc v Cybersell, Inc 130 F. 3d 414
- Dareportal, (2022) "*Digital Around the World*" *Dareportal* [Online], Retrieved [February 3, 2022] https://datareportal.com/global-digital-overview#:~:text=Internet%20use%20around%20the%20world,500%2C000%20new%20users%20each%20day
- Division of Industry and Community Universiti Sains Malaysia, (2013), 'Volunteerism in Malaysia', Penerbit Universiti Sains Malaysia, 1.
- Dunt I., (2018), "May Speech: Nice World, if Only We Lived in it" *Politics* [Online], [Retrieved February 3, *2022]* https://www.politics.co.uk/blogs/2018/10/03/may-speech-nice-world-if-only-we-lived-in-it/
- Economist, (2019), 'Globalisation has faltered: It is now being reshaped', The Economist 21.
- E-Governmental National Centre, (2010), "First Cybercrime Conviction in Brunei" *E-Government National Centre, Prime's Minister Office of Brunei Darussalam* [Online], [Retrieved February 8, 2022], <http://egncbrunei.blogspot.com/2010/05/first-cybercrime-conviction-in-brunei.html
- Frinklea K.M., (2013), 'The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S Law Enforcement' Congressional Research Service, 1.
- Gan R.Y., (2018), 'Brunei Cyberspace Masterplan 2018' ResearchGate, 4.
- Gray T.L., (2002) 'Minimum Contacts in Cyberspace: The Classic Jurisdiction Analysis in a New Setting' Journal of High Technology Law, 1(1), 86.
- Hanson v Denckla 357 U.S. 235, 253 (1958)
- Information Department, (n.d.), "About Brunei Darussalam", *Information Department, Prime Minister's Office*, [Online], [Retrieved February 8, 2022], http://www.information.gov.bn/SitePages/About%20Brunei%20Darussalam.aspx.
- International Shoe Co. v Washington 326 U.S 310 (1945)
- Legal Status of Eastern Greenland (Denmark v Norway) (1933) PCIJ Series A/B No. 53 at 48; Ryngaert C., (2015) Jurisdiction in International Law, Oxford University Press, 2nd edn., 26.
- Lewis J. and Roth A., (2019) "Russia's Great Firewall: Is it meant to keep information in or out?" *The Guardian* [Online], [Retrieved February 4, 2022] https://www.theguardian.com/technology/2019/apr/28/russia-great-firewall-sovereign-internet-bill-keepinginformation-in-or-out/
- Liaropoulos A., (2013) 'Exercising State Sovereignty in Cyberspace: An International Cyber Order under Construction?', Journal of Information Warfare, 12(2), 19.
- Maier B., (2018) 'How Has the Law Attempted to Tacke the Borderless Nature of Internet?' International Journal of Law and Information Technology, 18 (2), 142.
- McDonald N., (2018), "*Digital in 2018: World's Internet users pass the 4 billion mark*", *We are Social* [Online], [Retrieved February 4, 2022],

https://wearesocial.com/us/blog/2018/01/global-digital-report-2018/

- Mohamed D., (2012), 'Investigating Cybercrimes under the Malaysian Cyber laws and the Criminal Procedure Code: Issues and Challenges' Malayan Law Journal, 6(i), 5.
- McGee v International Life Insurance Co. 355 U.S 220 (1957)
- Ryder R.D., (2001), Guide to Cyber Laws (Informational Technology Act, 2000, E-Commerce, Data Protection and the Internet, 1st edn., Wadhwa & Co Law Publishing Co, Nagpur, 207
- Saakashvili E., (2019) "The Global Rise of Internet Sovereignty" *Coda* [Online], [Retrieved February 4, 2022], https://www.codastory.com/authoritarian-tech/global-rise-internet-sovereignty/
- Sachdeva A.M., (2007), 'International Jurisdiction in Cyberspace: A Comparative Perspective' Computers and Telecommunication Law Review, 8, 246.
- Sharbawi Z., (2011), "The 11th China-ASEAN Prosecutors-General Conference" *Attorney General Chamber of Brunei Darussalam* [Online] [Retrieved February 9, 2022] https://www.agc.gov.bn/conference/Secretariat%20Documents/Speech%20and%20Key%20Notes/Brunei%20Key%20Note%20Speech%2011%20CAPGC.pdf