بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# CYBERLAWS IN BRUNEI DARUSSALAM AND SINGAPORE: A COMPARATIVE ANALYSIS

**AZILLA LIYANA BINTI MOHD AZAM ZAKI**
**18MR608**

**FACULTY OF SHARIAH AND LAW**
**UNIVERSITI ISLAM SULTAN SHARIF ALI**
**BRUNEI DARUSSALAM**

**1442H/2021M**

# CYBERCRIME: A COMPARATIVE STUDY OF THE DEVELOPMENTS OF CYBERLAWS IN BRUNEI AND SINGAPORE

**AZILLA LIYANA BINTI MOHD AZAM ZAKI**

**18MR608**

**A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF LAWS OF RESEARCH**

**Faculty of Shariah and Law**

**Universiti Islam Sultan Sharif Ali**

**Negara Brunei Darussalam**

**Rajab 1442 / March 2021**

**SUPERVISION**

CYBERLAWS IN BRUNEI DARUSSALAM AND SINGAPORE: A COMPARATIVE ANALYSIS

**AZILLA LIYANA BINTI MOHD AZAM ZAKI**

**18MR608**

**Supervisor: _____**

**Signature: _____ Date: _____**

**Faculty Dean: _____**

**Signature: _____Date:_____**

**DECLARATION**

بسم الله الرحمن الرحيم

**I hereby declare that the work in this academic exercise is my own except for quotations and summaries which have been duly acknowledged.**

**Signature:**

**Name:** Azilla Liyana Binti Mohd Azam Zaki

**Registration Number:** 18MR608

**Date of Submission:** 20 Rajab 1442/ 4 March 2021

**DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE ON UNPUBLISHED RESEARCH**



**CYBERLAWS IN BRUNEI DARUSSALAM AND SINGAPORE: A COMPARATIVE ANALYSIS**

## ACKNOWLEDGEMENT

Praise be to Allah SWT Who has never fail to fulfil His SWT covenant to all of us. The appreciation is due to Dr Ahmad Ma'sum, supervisor of this academic exercise for his continued support and guidance during the writing of this thesis. His patience, understanding and wisdom throughout this journey should be commended and I am grateful for him. My special thanks is due to the Government of His Majesty, Sultan Haji Hassanal Bolkiah Mu'izzaddin Waddaulah, Sultan dan Yang Di-Pertuan of Brunei Darussalam, who granted me a scholarship and hence, enabled me to pursue my study at Universiti Islam Sultan Sharif Ali. This extends to the Faculty of Shari'ah and Law of the Universiti Islam Sultan Sharif Ali, the Attorney General's Chambers and the Brunei Judicial Courts for their assistance in guiding me throughout this research. A dedication is also extended for my father, Mohd Azam Zaki bin Haji Mohd Zain, for his relentless and unconditional love and support for me to achieve my dreams. He is the very reason why I am here today.

## ABSTRACT

### CYBERLAWS IN BRUNEI DARUSSALAM AND SINGAPORE: A COMPARATIVE ANALYSIS

The rate of cybercrime is increasing exponentially for the last few years and has shown great concern on the part of the Bruneian government. Brunei's cyberlaws are insufficient to cope with cybercrime which keeps evolving rapidly with technology. Singapore is a pioneer in cybercrime and has been of great assistance to Brunei during times where Brunei needs to amend her laws in the past. The objective of this research is to study the historical development of cybercrime in Brunei and Singapore as well as to comparatively analyse the laws dealing with cybercrime in Brunei and Singapore. In doing so, this research observes the extent Singapore's cyberlaws are adoptable in Brunei. In terms of research methodology, the research adopts a doctrinal legal research approach. Apart from adopting the doctrinal legal research approach, the research also analyses the data collected by using both analytical and comparative methods of data analysis. As to the findings, the research concludes that Singapore legislations as the standard and guidance for Brunei legislation. The research recommends that there should be a consistency in amending the Brunei legislations as well as a systemized structure for cybersecurity enforcers.

# ABSTRAK


**UNDANG-UNDANG SIBER DI BRUNEI DARUSSALAM DAN SINGAPURA: ANALISIS PERBANDINGAN**

Adapun statistik kadar jenayah siber selang beberapa tahun kebelakangan ini menampakkan peningkatan secara mendadak lantas mendapat perhatian besar dari pihak kerajaan Brunei. Undang-undang siber Brunei tidak mencukupi untuk menangani jenayah siber yang terus meningkat selari dengan berkembangnya teknologi. Singapura sebagai negara pelopor di dalam jenayah siber telah banyak membantu Brunei terutama sekali di dalam perihal pemindaan undang-undangnya yang lalu. Objektif penyelidikan ini adalah untuk mengkaji sejarah perkembangan jenayah siber di Brunei dan Singapura serta menganalisis perbandingan undang-undang yang berkaitan dengan jenayah siber kedua-dua buah negara tersebut. Dengan itu secara tidak langsung penyelidikan ini dibuat adalah melihat sejauh mana undang-undang siber Singapura dapat diterimapakai di Brunei. Dari segi metodologi penyelidikan, kajian ini menggunakan pendekatan penyelidikan hukum doktrin. Selain itu, penelitian ini juga menganalisis data yang dikumpulkan dengan menggunakan kedua-dua kaedah analisis data dan perbandingan. Mengenai penemuan itu, penyelidikan menyimpulkan bahawa perundangan Singapura sebagai piawaian dan panduan untuk perundangan Brunei. Penyelidikan ini mengesyorkan agar ada konsistensi dalam mengubah perundangan Brunei dan juga struktur sistematik untuk penguatkuasa keselamatan siber.

## ملخص البحث

### مقارن تحليل :وسنغافورة السلام دار بروه ي في الإلكترونية الجريمة

يتزيد معدل الجرائم الإلكترونيه بشكل كبير خلال السنوات القليلة الماضيه وأظهر لدًا كبيرً من جانب حكومة بروناي. قوانين الإلكترونية لبروناي غير كافية للتعامل مع الجرائم الإلكترونية التي تتطور بسرعة مع التكنولوجيا. يتزيد معدل الجرائم الإلكترونيه بشكل كبير خلال السنوات القليلة الماضيه وقد أظهر لدًا كبيرً من جانب حكومة بروناي. وقد سنغافورة دولة رائدة في مجال الجرائم الإلكترونيه وقد لعبت مساعدة كبيرة لبروناي خلال الأوقات التي تحتاج إليها بروناي لأجل تعديل قوانينها في الماضي. الهدف من هذا البحث هو دراسة التطور التاريخي للجرائم الإلكترونية في بروناي وسنغافورة وكذلك تحليل القوانين التي تتعامل مع الجرائم الإلكترونية في بروناي وسنغافورة. من خلال القيام بذلك، يلاحظ هذا البحث مدى قابلية قوانين الإلكترونيه لسنغافورة في بروناي. من حيث منهجية البحث يتبنى البحث منهج البحث الدستوري القانوني بصرف النظر عن اعتماد نهج البحث القانوني الدستوري، يحلل البحث أيضًا الإجابات التي تم جمعها باستخدام منهجي التحليل والمقارن لتحليل البيانات. فيما يتعلق بالنتائج، خلص البحث إلى أن تشريعات سنغافورة هي المعيار والمرجعية لتشريعات بروناي. تقترح الباحثة بضرورة أن يكون هناك تناسق في تعديل تشريعات بروناي بالإضافة إلى ترتيب منظم لجهات إنفاذ الأمن الإلكتروني.

**TABLE OF CONTENTS**

## LIST OF ABBREVIATIONS

| | |
|---|---|
| AGC | Attorney General's Chamber |
| ATM | Automated Teller Machine |
| AMBD | Autoriti Monetari Brunei Darussalam |
| AP-CERT | Asia Pacific Computer Emergency Response Team |
| ASEAN | Association of Southeast Asian Nations |
| BIBD | Bank Islam Brunei Darussalam |
| BCMA | Brunei Computer Misuse Act 2007, Chapter 194 |
| BruCERT | Brunei Computer Emergency Response Team |
| CFAA | Computer Fraud and Abuse Act of 1986 |
| CID | Criminal Investigation Department |
| CII | Critical Information Institute |
| CJD | Criminal Justice Division |
| CSA | Cybersecurity Agency Singapore |
| DDoS | Distribute Denial of Service |
| DNC | Democratic National Committee |
| ECMA | English Computer Misuse Act 1990, Chapter 18 |
| Ed. | Edition |
| *et al* | And others |
| FBI | Federal Bureau Investigation |
| FIRST | For Inspiration and Recognition of Science and Technology |
| HSBC | Hong Kong – Shanghai Bank Corporation |
| ICT | Information Communication Technology |
| IP | Intellectual Property |
| IT | Information Technology |
| ITPSS | Informational Technology Protective Security Services Sdn Bhd |
| ITU | International Telecommunication Union |
| MINDEF | Ministry of Defence |
| MIT | Massachusetts Institute of Technology |
| NDA | Non-Disclosure Agreement |
| No. | Number |
| OA | Official Assignee |
| OIC-CERT | Computer Emergency Response Team for Organisation of Islamic Cooperation |
| p. | Page |
| para. | Paragraph |
| pp. | Pages |
| RBAF | Royal Brunei Armed Force |
| RBPF | Royal Brunei Police Force |
| SCMA | Singapore Computer Misuse Act 1993, Chapter 50A |
| SMEs | Small and Medium Enterprises |
| TBA | Takaful Brunei Am Sdn Bhd |

| | |
|---|---|
| UK | United Kingdom |
| UOB | United Overseas Bank |
| US | United States |

**LIST OF CASES**

## LIST OF STATUTES

**Laws of Brunei**

Brunei Computer Misuse Order 2000

Brunei Computer Misuse Act 2007, Chapter 194

Brunei Criminal Procedure Code 2001 (Brunei Criminal Procedure Code), Chapter 7

Brunei Penal Code 1957, Chapter 22

**Other Laws**

Computer Fraud and Abuse Act of 1986, 18 U.S. Code § 1030

Cybersecurity Act 2018 (No. 9 of 2018)

English Computer Misuse Act 1990, Chapter 18

Malaysia Penal Code 1936, Act 574

Undesirable Publications Act 1967, Chapter 338

Singapore Computer Misuse 1993, Chapter 50A

Singapore Criminal Procedure Code 2010 (No. 15 of 2010)

Singapore Penal Code 1871, Chapter 224

Singapore Evidence Act 1893, Chapter 72

# CHAPTER 1

# INTRODUCTION

## 1.1 Background of the Study

Cybercrime is a computer crime "a crime involving the use of a computer, such as sabotaging or stealing electronically stored data."[1] According to Cybersecurity Ventures, there will be at least $6 trillion of cybercrime damages by 2021.[2] In the foreword by Micheal Sullivan in "Cyber Threat! How to Manage the Growing Risk of Cyber Attacks", he opined that Thomas Alva Edison's quote "genius is 1% inspiration and 99% perspiration" does not apply in this matter; but instead, it is 99% preparation and 1% perspiration.[3] In the late 1980s, the infamous virus, namely, "Trojan" was distributed through a floppy disk by a company calling itself "PC Cyborg".[4] The Trojan encrypted the contents of the victim's hard disk after 90 re-boots, leaving just a "README" file containing a bill and an address in Panama to which payment was to be sent. Dr Joseph Popp, the alleged author of the Trojan, was later extradited to the UK to stand trial on charges of blackmail and damaging computer systems. However, he was released on the ground that he was unfit to stand trial due to mental health issues.

---

[1] Thananchayan, V. S. S. (2019, May 28). *Computer Crimes And Cybercrimes: A Critical Analysis Focusing On Sri Lanka*. Law Man, Retrieved August 1, 2020 from http://www.lawmanlanka.com/blog/Public%20and%20International%20Law/59#:~:text=As%20per%20Black's%20Law%20Dictionary,and%20it%20needs%20internet%20connection.

[2] Morgan, S. (2016, October 16). *Cybercrime Damages $6 Trillion by 2021*. Cybercrime Magazine, Retrieved August 30, 2020 from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[3] See foreword by Michael Sullivan. Ulsch, M. (2014). *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks*. Wiley Corporate F&A.

[4] Simone, A. (2015). *The Strange History of Ransomware*. Medium, Retrieved May 30, 2020 from https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b.

In 2010, Brunei saw the prosecution of its first cybercrime case. The defendant was charged under Section 6(1)(a) of the Brunei Computer Misuse Act 2007, Chapter 194 where he hacked into a wireless Internet connection without authorisation and using a stolen credit card number to make online purchases without the owner's knowledge and authority. The defendant was convicted and sentenced to 28.5 months imprisonment in total.[5] It was reported that Brunei had the highest Instagram penetration in the world, with 63% of the population above 13-years-old using the photo and video sharing platform.[6] It saw an increase by 14% to 220,000 users in the past year and this competes with more than 230 countries. On the other hand, Twitter showed a decrease of 4.6% while LinkedIn grew by 5.9%. Males make up the majority of Bruneian social media users on Facebook (57%), Twitter (64%) and LinkedIn (60%) with the exception of Instagram, whose user base is 55% female.[7] There were not many surveys conducted inorder to check and balance the consequences of the rising penetration into the Internet nor were there official records of complaints provided. However, there is a record that the number of cybercrime in Brunei increased year after year. A total of 2,143 cybersecurity attacks were recorded in Brunei in 2017 alone.[8]

New developments in Information Technology (IT) also provide new opportunities for offenders, a problem which already challenges and will continue to challenge, the criminal law system. The Attorney General Yang Berhormat Dato Paduka Hj Hairol Arni Hj Abdul Majid, in his Legal Year 2019, speech said that the "[the] Attorney General's Chambers (AGC) is working closely with other government agencies to draft new legislations on monitoring and more efficient reporting of cybersecurity threats. The new laws will also create a licensing regime that will regulate how data security is handled."[9] It further adds dimension to data privacy, cybercrime legal framework and cybersecurity. The AGC is committed in raising awareness of this new

[5] HITBSECNEWS. (2010, May 6). *First Cybercrime Conviction in Brunei*. HITBSecNews, Retrieved June 9, 2020 from https://news.hitb.org/content/first-cybercrime-conviction-brunei.
[6] Wong, A. (2019, April 29). *Brunei's Instagram penetration highest in the world.* BIZ BRUNEI, Retrieved May 30, 2020 from https://www.bizbrunei.com/2019/04/bruneis-instagram-penetration-highest-in-the-world/.
[7] Wong. *Brunei's Instagram penetration highest in the world.*
[8] Wong. *Brunei's Instagram penetration highest in the world.*
[9] Speech by Yang Berhormat Dato Paduka Haji Hairol Arni Bin Haji Abdul Majid, Attorney General, at the opening of Legal Year 2019, Retrieved June 19, 2019 from http://www.agc.gov.bn/AGC%20Images/downloads/speech/Legal%20Year%202019.pdf.

crime by strengthening enforcement in order to ensure that our nation and population are protected. Its strategies are as follows:

1. establishing the Cybersecurity Working Group to coordinate information sharing and formulate joint action to address and cybersecurity matter that led to the creation of the Brunei Darussalam National Cybersecurity Framework; and
2. the setting up of a Cybercrime Focus Group by the Attorney General that aims to continuously study and research international best practices while ensuring our laws are compliant with international standards; and creating a strong legal framework in any national strategy to address cybercrime.[10]

In Singapore, there have been many amendments made to the Computer Misuse Act 1993, Chapter 50A, ever since it was enacted in 1993. In 2014, after the infamous attack by "the Messiah", a computer hacker, onto government infrastructure systems, the lawmakers included provisions on cyberattacks on Critical Information Institutes (CII).[11] However, in 2018, a separate legislation was enacted focusing on the CII while further amendments were made to the respective Computer Misuse Act. This new legislation is the Cybersecurity Act 2018 (No. 9 of 2018) (Cybersecurity Act 2018). It is an initiative to level up the digital security and digital resiliency across industry sectors that provide essential services in Singapore. The cyber-statute provides framework to CII owners on their obligations to proactively protect their data and networks from cyberattacks. Indeed, the law evolves as cybercrime evolves.

Brunei is still lacking in her cyberlaws and IT system. Her existing criminal laws are still insufficient to cover the newly emerged forms of cyber wrongdoing. Research has identified the limited effectiveness of the current Bruneian cyber legislations in tackling cyber wrongdoing by not expanding its scope to include other factors that

[10] Syazwani Hj Rosli. (2018, August 15). *Brunei minister calls for vigilance against new cyber threats*. Borneo Bulletin, Retrieved April 15, 2019 from https://borneobulletin.com.bn/minister-calls-for-vigilance-against-new-cyber-threats/.

[11] Poh, I. (2015, January 30). *Hacker who called himself 'The Messiah' jailed 4 years and 8 months*. The Straits Times, Retrieved May 30, 2020 from https://www.straitstimes.com/singapore/courts-crime/hacker-who-called-himself-the-messiah-jailed-4-years-and-8-months.

contribute to the respective wrongdoing.[12] Marco et al argued that Brunei's cyber-statutes are insufficient to cope with cybercrime which keeps evolving rapidly with technology.[13]

In general, this research is written in reflection of the AGC of Brunei's initiative to amend the cybercrime law in Brunei. The research has focussed on the development in legislations and approaches taken in both Brunei and Singapore, its rationale for amendments and its application. For example, Brunei's cyber legislation, when compared to Singapore has a huge gap in advancement. Brunei is ready to enter into the IT arena where all transactions and work are done through the use of technology. The country is ready to become a Smart Nation and thus, it is significant for Brunei to look towards Singapore, a country known to be a Smart Nation as well, to assist in amending her laws. This research has explored and compared the Brunei and Singapore cyber legislations and discussed how the Singaporean legislation may be of assistance to Brunei in terms of amending its own cyber-statute.

### 1.2 Reason for Topic Selection

There are various reasons why the researcher has chosen this topic for her research. One of them is due to AGC's mission to amend Brunei's cyber legislations to combat the ongoing rise of cybercrime in the country. Further, Brunei is aiming to become a Smart Nation as well.[14] This brings to mind of Singapore, a Smart Nation whose cyberlaws have been constantly amended to suit its cybercrime challenges. Therefore, Singapore has been chosen for a comparative study with Brunei on their cyber legislations and approaches.

### 1.3 Problem Statement

[12] Marco, B., *et al*. (2018). *Brunei Cybersecurity Masterplan 2018*. S. Rajaratnam School of International Studies. p. 14.
[13] Marco. *Brunei Cybersecurity Masterplan 2018*.
[14] Wardi Wasil. (2020, February 7). *Brunei records nearly 40 per cent increase in cybersecurity attacks*. The Bruneian News, Retrieved May 31, 2020 from https://www.thebruneian.news/brunei-records-nearly-40-per-cent-increase-in-cybersecurity-attacks/.

In accordance with the research title and the background of the study, it is of paramount importance to note that the main problem faced by Brunei is that the lack of cyberlaws to deal with or combat the increasing cybercrimes. According to Christopher Ng, a Deputy Public Prosecutor at the Criminal Justice Division of the AGC, he said that "[c]ybercrime is evolving, therefore laws need to evolve, too. We feel that cyber stalking, online harassment, phishing are currently not appropriately covered and we will need to look into the amendments of our laws in the future."[15] In Brunei, the challenges that the prosecutors have to face are the lack of cyberlaws inorder to combat the increasing cybercrimes. The rate of cybercrime is increasing exponentially for the last few years and has shown great concern on the part of the Bruneian government. Although there were efforts to warn the public about the dangers of being less prudent with regards to cybersecurity, there is a need to show great commitments to her laws and policies.

Unlike Singapore where cyberlaws are of top priority, Brunei lacks cybersecurity in her laws and IT system. It needs consistency when it comes to amending the legislations to suit the present situation. There is limited effectiveness of the current Bruneian cyber legislations in tackling cyber wrongdoing due to its limited scope.[16] Marco et al conjectured that Brunei's cyberlaws are insufficient to cope with cybercrime which keeps evolving rapidly with technology.[17] The Brunei Computer Emergency Response Team (BruCERT) was formed in 2004 and is Brunei's first trusted one-stop referral agency in dealing with computer-related and Internet-related security incidents in Brunei.[18] It is the central hub that coordinates with international Computer Emergency Response Team (CERT), network service providers, security vendors, government agencies, as well as other related organisations to facilitate the detection, analysis and prevention of security incidents on the Internet. Through a global affiliation with other CERTs, BruCERT acquires valuable information on IT security threats and shares findings on security risks detected within the nation's IT infrastructure. These findings are made publicly accessible with the objective of

[15] Abdul Aziz Ismail. (2016, May 31). *AGC, RBPF link arms to fight cybercrime*. BT Archive, Retrieved August 8, 2020 from https://btarchive.org/news/national/2016/05/30/agc-rbpflink-arms-fight-cybercrime.
[16] Abdul Aziz Ismail. *AGC, RBPF link arms to fight cybercrime*.
[17] Abdul Aziz Ismail. *AGC, RBPF link arms to fight cybercrime*.
[18] *About BruCERT*. BRUCERT. Retrieved June 6, 2020 from https://www.brucert.org.bn/node/1.

increasing IT Security awareness. Although BruCERT does its job at protecting computers against cyberattacks, there is a need in attentiveness on the increasing diverse of cyberbreach.

### 1.4 Research Questions

This research, through comparative study, intends to answer three research questions:

1. What is the historical development of cybercrime in Brunei and Singapore?
2. How to comparatively analyse the laws dealing with cybercrime in Brunei and Singapore?
3. Should Brunei adopt the same laws dealing with cybercrime as Singapore's?

### 1.5 Research Objectives

The research objectives can be divided into three steps corresponding to the abovementioned sub-research questions:

1. To study the historical development of cybercrime in Brunei and Singapore.
2. To comparatively analyse the laws dealing with cybercrime in Brunei and Singapore.
3. To recommend the extent that Brunei should adopt the same laws dealing with cybercrime as Singapore.

### 1.6 Significance of the Study

The significance of this study is to identify the factors contributing to the broader problems in cybercrime. This study will be beneficial to the development of the cyberlaws in Brunei as Brunei is moving towards moulding into a Smart Nation – like Singapore. The study will provide government agencies, educational institutes, academia as well as the legal arena an indepth understanding of cybercrime and its functions. In understanding this innovating concept, the study implores an understanding of the issues and problems arised from cybercrime. In order to relieve

some of these issues and problems, the recommendation provided by this study will assist them in improving Brunei's laws in handling cybercrime. Further, this research will be a stepping stone for others to research more into this topic in order to assist Brunei's vision to be at par at the global level. This is an inevitable topic and needs to be reviewed in the coming future as the cyber world innovates. Viewing the history of cybercrime, it is not novel per se, yet its growth, expansion and variant productions are what makes it novel every single time. Brunei understands this and this is reflected in her efforts to curb this growing menace. Singapore is indeed a pioneer in cybercrime and in essence, has been of great assistance to Brunei during times where Brunei needs to amend her laws in the past.

In this light, the researcher hopes that this research would be able to benefit Brunei to better her regulations on cybercrime. This research believes that it will indeed be of good guidance. After 12 years, the AGC has initiated to amend the cyberlaws. It is good news and in light of this good news, the researcher hopes the conclusions and recommendations proposed in this research would be able to assist AGC and other government sectors in amending their laws.

**1.7 Research Methodology**

In order to examine the cybercrime legislations of Brunei and Singapore, the method of doctrinal research has been used. Doctrinal research can be defined in a simple way as 'research which asks what the law is in a particular area.'[19] It is the method most consistently used when a research intends to investigate and analyse a body of law, including case law and relevant legislation, which are the primary sources and journal articles or other written commentaries on the jurisprudence and legislations, categorised as, the secondary sources. It is library-based research that seeks to find the "one right answer" to certain legal issue or questions. Further, analytical and comparative methods were employed in this research as well. Cybercrime legislations, literatures and case laws are examined to answer the above questions. Here, the application of the legislations, the issues addressed, and the opinions from the academia, jurisdiction and the legislature can be explored. The materials accumulated

[19] McConville, M., *et al*. (2007). *Research Methods for Law*. Edinburgh University Press. pp. 18-19.

from the previous research can contribute to identifying and analysing the similarities and divergences among the approaches taken by the selected legal regimes.

It is worth noting that the legislative taken by a selected legal regime is sometimes complex, and some special regulations on jurisdiction and enforcement power may also reflect its features. In such cases, relevant criminal procedural issues are also addressed if their discussion can contribute to understanding the unique approach taken by the selected legal regime.

Research for materials has been carried out in archives or library of AGC, Brunei Supreme Court, Universiti Brunei Darussalam and Universiti Islam Sultan Sharif Ali. Attachment programmes has been conducted at the AGC's Criminal Justice Division and the Legal Drafting Division for the purpose of clarifying the researcher's understanding of the laws and gaining indepth information on cybercrime.

**1.8 Research Scope and Limitations**

For a better understanding of cybercrime legislations and to contribute to the betterment of cybercrime regulations, this research has chosen two jurisdictions for its comparative research - Brunei and Singapore. The advancement of the Singaporean legal legislations on cybercrime is the main reason for choosing Singapore as a comparison subject. Given that the legal traditions and societal cultures of Singapore and Brunei are similar, and thus of comparability, Singapore was selected based upon these reasons. For another, both countries share the same issues and considerations when adapting the criminal law to address cybercrime. In addition, much material on Singaporean cybercrime legislation in English law is available for comparison, including the legislation, parliamentary discussion and academic analysis. However, the research also made reference to other jurisdictions such as the United Kingdom (UK), Australia and Malaysia. The purpose is to provide a larger context in the arguments provided in this research. Further, these countries share the same law the common law.

Singapore's cybercrime legislations are based on the English laws. The provisions in the Singapore Computer Misuse Act 1993, Chapter 50A (SCMA) are borrowed directly from the English Computer Misuse Act 1990, Chapter 18. Brunei is not far from its similarities with the Singapore legislation; it has always relied on Singapore legislations as reference and guidance during the time of the amendments of her own laws.

This research has looked into the origins and evolution of cybercrime legislation in the selected legal regimes, the cyber legislations in Brunei and Singapore, the judicial approaches that have been taken in the field of the criminal law in relation to cybercrime and the issues that they have addressed and how criminal law are adapted to regulate cybercrime, judicial approaches, and finally, the counter measures taken by these two countries to tackle cybercrime.

As for the limitations, it should be mentioned that there are little research or publications on Brunei's cybercrime legislations although the issue has been raised so many times by relevant authorities throughout the years.[20] No official document is available from the government institutions pertaining to cybercrime thus literature sources attained for this research relied on published law journals and online news articles. However, it is noteworthy to state that the published law journals available, i.e., the Singaporean Law Journals, in Brunei are not updated and there are few and brief published law articles on cybercrime in Brunei from the Internet. For this research, the Brunei cybercrime cases were mostly obtained through the use of the Brunei Judiciary website.[21] Here, only Intermediate Courts, High Courts and Courts of Appeal cases are published. Magistrate Courts cases are not available for the public to view. Most of the cybercrime cases held in Brunei are under Magistrates Courts. For the case of Singapore, although courts cases are published in their Judiciary website[22] for public view, there are not many cybercrime cases available to be viewed. The website only allows full access if one subscribes to the website, which is costly.

[20] Ain Bandial. (2018, August 14). *AG: Strengthen Current Laws to Address Current Issues*. The Scoop, Retrieved September 11, 2019 from https://thescoop.co/2018/08/14/ag-strengthen-current-laws-to-address-new-cyber-threats/.
[21] *Judiciary*. State Judiciary Department, Brunei Darussalam. Retrieved September 11, 2019 from www.judiciary.gov.bn.
[22] Supreme Court, Singapore. Retrieved September 11, 2019 from www.supremecourt.gov.sg

Published journals are not available in the website as well. Thus, United States, UK, Australian and Malaysian legislations and cases were referred to as means to elaborate more on some points in this research.

**1.9 Literature Review**

Kshetri said that it is unclear whether cybercrime refers to legal, sociological, technological, or legal aspects of crime and a universal definition remains elusive.[23] However, the definition of the "cybercrime" is demonstrated in Jiow where he stated that the computer can be an instrument or tool used to perpetuate a crime and that these acts are classified as "old crimes using new tools" or "new crimes using new tools".[24] Mcguire et al had termed this definition differently - "old crimes using new tools" as "cyber-enabled crimes" and "new crimes using new tools" as "cyber-dependent crimes." In Brunei, her cyberlaws are lacking, Marco et al argued that Brunei's cyber-statutes are insufficient to cope with cybercrime which keeps evolving rapidly with technology.[25] Pg Ibnu found that at least 13% have had experienced identity theft. The study also indicated that at least 24% of the users have had their computers hacked although only 93% said their phones have never been hacked. As computers or technology innovates, cybercrime innovates too. The increase of cybercrime was highlighted by Mr Wong Kang Seng where he said that it is necessary to update the Computer Misuse Act to deal with an increasingly complex environment.[26]

In Brunei and Singapore cyber legislations, the fundamental element distinguishes between a cybercrime and a normal criminal crime is the computer element in the commission of the crime. In defining 'computer', Wong states that there are two ways: providing an all-inclusive definition while at the same time listing certain devices that cannot be regarded as a computer or leaving the term 'computer'

[23] Kshetri, N. (2010). Global Cybercrime Industry: Economic, institutional and strategic perspectives. Berlin Heidelberg: Springer Science & Business Media.
[24] Jiow, H. J. (2013). *Singapore's Cybercrime Regulation based on Lessig's Modalities of Constraint*. International Journal of Cybercriminology. p. 4.
[25] Marco, B., *et al*. (2018). *Brunei Cybersecurity Masterplan 2018*. S. Rajaratnam School of International Studies. p. 14.
[26] *Second Reading of the Computer Misuse (Amendment) Bill.* (1998, June 30). (No. 24/1998).

**BIBLIOGRAPHY**


Ahmed, S.R. (2020). *Preventing Identity Crime: Identity Theft and Identity Fraud: An Identity Crime Model and Legislative Analysis with Recommendations for Preventing Identity.*

Aravinthan, G. (2010, June 7). *Nature of Copyright infringement in Internet*. Lawyers Clubs India, https://www.lawyersclubindia.com/articles/nature-of-copyright-infringement-in-internet-2953.asp.

Ashworth, A. (2015). Sentencing and Criminal Justice. 5th Ed. *Cambridge University Press.*

Awan, I., *et al*. (2015, December 18). *Virtual and Physical World Anti-Muslim Hate Crime*. The British Journal of Criminology.

Back, M.D., *et al.* (2010). *Facebook profiles reflect actual personality, not self-idealization*. Psychological Science.

Black, H.A. (1990). ***Black's Law Dictionary***. 6th Ed. St. Paul, Minn. West Publishing Co.

Bowker, A *et al*. (2003). *An introduction to the supervision of the cybersex offender*. Federal Probation.

Bromby, M. (2006). *Security against Crime: Technologies for Detecting and Preventing Crime.* International Review of Law Computer & Technology.

Brown, C. S. D. (2015). *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice.* International Journal of Cybercriminology. Volume 9.

Burnap, P. *et al*. (2015). *Cyber Hate Speech on Twitter: An application of Machine Classification and Statistical Modeling for Policy and Decision Making.* Policy and Internet Crime. Brill

Caplan, J., *et al*. (2001). *Documenting individual identity*. Princeton, NJ: Princeton University Press.

Craig, B. (2012). *CyberLaw The Law of the Internet and Information Technology*. Pearson.

Christopherson, K. (2007). T*he Positive and Negative Implications of Anonymity in Internet, Nobody Knows You're a Dog*. Computers in Human Behaviour.

Dashora, K. (2011). *Cyber Crime in the Society: Problems and Preventions,* Journal of Alternative Perspectives in the Social Sciences (2011).

Desai, D. A., Jain, M.L, Madhava Menon, N.R. (1995). ***Ratanlal and Dhirajlal's Law of Crimes***. 23rd Ed. Bharat Law House.

Dk Noryoul Elia Fatimah Pg Ibnu. (2011). *Cybercrime in Brunei: Lessons Learnt From Malaysian Perspectives*. Universiti Brunei Darussalam.

Dombrowski, *et al*. (2004), *Protecting Children From Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations*. Professional Psychology: Research and Practice 2004.

*First reading of the Computer Misuse (Amendment) Bill* (2017, March 9) (No. 15/2017).

Ferrera, G.R and *et al.* (2011). *CyberLaw Text & Cases, South-Western's Special Topics Collection*. 3rd Ed. South-Western College/West.

Fletcher, N. (2007). *Challenges for regulating financial fraud in cyberspace*. Journal Financial Crime.

Geist, M. (2003). *Cyber Law 2.0*. Boston College Law Review.
Global Forum on Digital Security For Prosperity. *Organisation for Economic Co-operation and Development*, https://www.oecd.org/digital/global-forum-digital-security/about/.
Gorian, E. (2020). Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection. *Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection*, https://www.researchgate.net/publication/332351766_Singapore's_Cybersecurity_Act_2018_A_New_Generation_Standard_for_Critical_Information_Infrastructure_Protection
Hall, B.H. (2007). *Patents and patent policy*. Oxford Review of Economic Policy.
Hall, N. (2013). *Hate Crime*. Cullompton: Willan Publishing.
Hart, H.L.A. (1961). *The Concept of Law*. Oxford: Oxford University Press.
Herrera-Flanigan, J. R., *et al.* (2010). *Cybercrimes: A Multidisciplinary Analysis*. Criminal Regulations. In S. Ghosh & E. Turrini (Eds.). Berlin.
Higgins, E. *et al* (2008). *Digital Piracy: An Examination of Three Measurements of Self Control*. Deviant Behaviour.
Hewson, C., *et al.* (2003). *Internet research methods: A practical guide for the behavioural and social sciences*. London: Sage.
Hirsh, A. V. (1986). *Deservedness and Dangerousness in Sentencing Policy*. Criminal Law Report
ITPSS http://www.itpss.com/.
Jaishankar, K. (2008). *Cyber Hate: Antisocial networking in the Internet*, The International Journal of Cyber Criminology (IJCC).
Jarva, O. (2018, April 8). *What you need to know about the Singapore Cybersecurity Bill*. Network Asia.
Jiow, H.J. (2013). *Singapore's Cybercrime Regulation based on Lessig's Modalities of Constraint*. International Journal of Cybercriminology.
Joseph, B. (2017). *Digital Crime Investigation: Handbook for Cybercrime Investigators*. Independently published.
Judiciary. State Judiciary Department, Brunei Darussalam. www.judiciary.gov.bn
Keats, C.D., & *et al.* (2011). *Industrial Relations and the Law: retrospect and prospect*. British Journal of Industrial Relations.
Keyser, M. (2003). *The Council of Europe Convention on Cybercrime*. J. Transnational Law & Policy.
Khairun-Nisaa Asari, *et al.* (2014). *A Comparative Legal Analysis of Online Defamation in Malaysia, Singapore and the United Kingdom*. International Journal of Cyber-Security and Digital Forensics.
Koops, B.J, *et al.* (2006). *Identity Theft, Identity Fraud and/or Identity-related Crime*, Datenschutz und Datensicherheit.
Kshetri, N. (2010). Global Cybercrime Industry: Economic, institutional and strategic perspectives. Berlin Heidelberg: Springer Science & Business Media.
Lee, G.M.C. (1994). *Offences Created by the Computer Misuse Act 1993*. Singapore Journal of Legal Studies.
Magnus, R., *et al.* (2003). *Sentencing Practice in the Subordinate Courts*. 2nd Ed. Butterworths.
Marco, B., *et al.* (2018). *Brunei Cybersecurity Masterplan 2018*. S. Rajaratnam School of International Studies.
McCurdy, M.L. (2010). *Computer Crimes*. CRIM. L. REV.

Miller, R.L. (2007). *Business Law: Text & Cases An Accelerated Course*. 14th Ed. Cengage Learning.
Mustaine, E.E *et al*. (1999). *A routine activity theory explanation for women's stalking victimizations*. Violence Against Women.
Panetta, J. J., *et al*. (2015). *Cybersecurity Act of 2015 Review*. The Changing Faces of Cybersecurity Governance.
Parmar, A., *et al* (2016). *Critical Study and Analysis of Cyber Law Awareness Among the Netizens*. Proceedings of International Conference on ICT for Sustainable Development.
Purcell *et al* (2001). *The Management of Stalkers*. Advances in Psychiatric Treatment.
Rogers, W. V.H. (2010). *Winfield & Jolowicz on Tort*. 18th Ed. Sweet & Maxwell.
Rowland, J. B. (2002). *The role of automated detection in reducing cyber fraud*. The Journal of Equipment Lease Financing.
RMWARNER, http://kellywarnerlaw.com/brunei-defamation-laws/.
Ryder, R.D. (2007). *Guide to Cyber Laws (Information Technology Act, 2000 E-Commerce, Data Protection & The Internet)*, 3rd ed. Wadhwa and Company.
Sahu, S. S., *Et Al.* (2014). *Distributed Denial Of Service Attacks: A Review*, I.J. Modern Education And Computer Science 2014.
*Second Reading of the Computer Misuse (Amendment) Bill*. (1998, June 30) (No. 24/1998).
*Second Reading of the Computer Misuse Bill*. (1993, May 28) (No. 17/1993).
Sindhu, K. K., *et al*. (2012). Digital Forensics and Cyber Crime Datamining. Journal of Information Security.
Supreme Court, Singapore. www.supremecourt.gov.bn.
The Organisation for Economic Co-operation and Development (OECD). *Cybercrime Law*. Retrieved from https://www.cybercrimelaw.net/OECD.html
Ulsch, M. (2014). *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks*. Wiley Corporate F&A.
Urbas, G. (2008). *An Overview of Cybercrime Legislation and Cases in Singapore*. Asian Law Institute.
Walker, N. *et al* (1996), *Sentencing: Theory, Law and Practice*. 2nd Ed. *Butterworths*.
Wang, Q.Y. (2016), *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*, Wolf Legal Publishers.
Williams, M.L., *et al*. (2016). *Cyberhate on Social Media in the Aftermath of Woolwich: A Case Study in Computational Criminology and Big Data*. British Journal of Criminology.