A Review of Regulating Cybercrime in Singapore

Hee Jhee Jiow

Health & Social Sciences, Faculty Member, Singapore Institute of Technology, 10 Dover Dr, Singapore, Indonesia

jhee.jiow@singaporetech.edu.sg

Abstract. This paper is a commentary on my previous paper titled "Jiow, H. J. (2013). Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's four Modalities of Constraint. International Journal of Cyber Criminology, 7(1), 18-27. Retrieve from www.cybercrimejournal.com." Given that it was written 10 years ago, I sought to heuristically ascertain how far the effectiveness of the constraints have changed since the previous version.

Keywords: Cybercrime, Lessig's Modalities of Constraints, Effectiveness of the Constraints

1 Introduction

In 2013, I published a paper titled "Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's four Modalities of Constraint". It was largely a more theoretical piece than an empirical one, which claimed that social norms is the most effective constraint among the 4 modalities. And public education is the way to fashion such social norms.

Since then, there have been evolutions in technology and, how cybercrimes are committed in general. Specifically, Artificial Intelligence (AI) has been widely used in various types of cybercrime, such as the following (which is taken from [1]):

- Automated Attacks: AI can be used to automate various stages of cyber attacks, such as reconnaissance, intrusion, and data exfiltration. AI algorithms can quickly identify vulnerabilities and weaknesses in a target system and exploit them more efficiently than traditional methods.
- Phishing and Social Engineering: AI-powered chatbots or automated scripts can mimic human interactions, making phishing attacks more convincing. These attacks can trick individuals into divulging sensitive information or clicking on malicious links.
- Credential Stuffing: AI can automate the process of testing large lists of stolen usernames and passwords on various websites, identifying instances where users reuse passwords across platforms.

© The Author(s) 2023

M. Umiyati et al. (eds.), *Proceedings of the International Conference on "Changing of Law: Business Law, Local Wisdom and Tourism Industry" (ICCLB 2023)*, Advances in Social Science, Education and Humanities Research 804,
https://doi.org/10.2991/978-2-38476-180-7_56

- Malware Development: AI can be used to develop more sophisticated malware that can adapt to security measures, evade detection, and propagate within networks.
- Spear Phishing: AI can analyze publicly available data to create highly personalized spear phishing emails, making them more difficult to detect and increasing the chances of success.
- Evasion of Security Measures: AI can be used to analyze security systems and develop strategies to evade intrusion detection and prevention systems.
- Data Generation for Fake Content: AI-generated content can be used to create fake news, social media posts, or other types of misinformation to manipulate public opinion or spread disinformation.

Such evolution calls for relook into the regulation based on Lessig's Modalities of Constraints (LMC). However, in this instance, it would not be restricted to Singapore, as cybercrime's perpetrators may reside overseas.

2 Methods

As AI has been widely used as a tool for committing cybercrime, this paper will also adopt AI to explore regulation of cybercrime using Lessig's Modalities of Constraints. Specifically, it will adopt ChatGPT for this purpose. ChatGPT is an AI language model developed by OpenAI. It is popularly known and widely used. I will first (PART A) query ChatGPT on how regulation of cybercrime, adopting LMC, has evolved or changed over the 10 years, with the following statements "Discuss Singapore's regulation of cybercrime based on Lawrence Lessig's modalities of constraints" and "Discuss how Singapore's regulation of cybercrime has changed based on Lawrence Lessig's modalities of constraints". This will be a general query that is broad. Secondly (PART B), I will query ChatGPT on the different modalities specifically to explore the generated results. This will involve a question queried on each modality and a regeneration via ChatGPT. The 4 questions are:

a) Discuss how Singapore laws have evolved, over the last 10 years, to handle cybercrime.
b) Discuss how technology in Singapore have evolved over the last 10 years, to alleviate cybercrime.
c) Discuss how social norms in Singapore have evolved over the last 10 years, to discourage cybercrime.
d) Discuss how market forces in Singapore have evolved over the last 10 years, to discourage cybercrime.

3 Findings

PART A

The first answer to the first question by ChatGPT is shown below, with references to it.

“Singapore's regulation of cybercrime can be understood through Lawrence Lessig's modalities of constraints: law, norms, market, and architecture. Lessig's framework, as applied to Singapore's context, can involve legislative measures (law) such as the Computer Misuse Act, establishing social norms around responsible online behavior, utilizing market mechanisms to incentivize cybersecurity, and designing technical architectures to prevent and detect cybercrimes. The analysis of Singapore's cybercrime regulation based on Lessig's modalities has been explored in academic literature. The Singaporean government has employed various strategies, including legal provisions, public awareness campaigns, industry partnerships, and technological advancements, to create a comprehensive approach to combating cybercrime.

Footnotes

1. researchgate.net ↩
2. semanticscholar.org ↩
3. academia.edu ↩
4. lsecyberlaw.blogspot.com ↩” [2]

With regeneration of the results by ChatGPT, the following was obtained:

“Singapore's regulation of cybercrime can be analyzed using Lawrence Lessig's four modalities of constraints: law, norms, architecture, and market. The application of these modalities in Singapore's approach to cybercrime regulation has been studied by scholars like Jiow. Lessig's modalities emphasize how regulations are enforced in a digital environment.

Singapore's regulations on cybercrime include legal measures, such as the Computer Misuse Act, which criminalizes unauthorized access, data interference, and related offenses. Norms are also influential, as Singapore promotes cybersecurity awareness and education through campaigns and initiatives. Architectural constraints involve technical measures to secure critical infrastructure.

The market aspect involves economic incentives and disincentives, encouraging compliance and discouraging cybercriminal activities. Singapore's efforts to collaborate with industry stakeholders and provide a conducive business environment align with this modality.

In summary, Singapore's regulation of cybercrime combines legal, normative, architectural, and market-based approaches, aligning with Lessig's modalities to create a comprehensive strategy against cyber threats.” [2]

The first answer to the second question by ChatGPT is shown below:

“Singapore's regulation of cybercrime has evolved in line with Lawrence Lessig's modalities of constraints. The adoption of Lessig's four modalities—law, norms, architecture, and market—is reflected in the changes.

1. Law: Singapore enacted the Computer Misuse Act and other legislation to combat cybercrime.
2. Norms: Efforts like cybersecurity campaigns increased awareness and education.
3. Architecture: Technical measures were implemented to secure critical infrastructure and data.
4. Market: Incentives and disincentives were used to discourage cybercriminal activities and foster a secure digital environment.

These modalities continue to shape Singapore's approach, adapting to new cyber threats, technological advancements, and global trends. The country's regulatory strategy demonstrates a holistic response to cyber challenges.” [3]

The references highlighted are as shown below:

1. cybercrimejournal.com - An Analysis of Regulation based on Lessig's four ...
2. researchgate.net - Cyber crime in Singapore: An analysis of regulation based on Lessig's four modalities of constraint
3. academia.edu - Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's Four Modalities of Constraint
4. semanticscholar.org - Cyber Crime in Singapore: An Analysis of Regulation ... [3]

Upon regeneration of the second question, the following was shown:

“Singapore's regulation of cybercrime has evolved by adopting Lawrence Lessig's modalities of constraints. These modalities - law, norms, architecture, and market - have influenced changes in how cybercrime is addressed in Singapore:

Law: Singapore enacted the Computer Misuse Act and other legislation to criminalize cyber offenses.

Norms: The government promoted cybersecurity awareness and education to establish social norms against cybercrime.

Architecture: Technical measures were introduced to secure critical infrastructure and protect against cyber threats.

Market: Economic incentives were used to encourage compliance and discourage cybercriminal activities.

Over time, Singapore's approach has become more comprehensive and nuanced, with increased emphasis on collaborative efforts among government, industry, and the public. This aligns with Lessig's modalities, indicating a holistic strategy to address the evolving landscape of cyber threats.” [3]

The findings suggest that research into Singapore’s regulation of cybercrime (using Lessigs Modalities of Constraints) has not changed much over the years. Results generated have been referencing the paper that I wrote.

PART B

The first answer to the first question by ChatGPT is shown below, with references to it.

“Over the past decade, Singapore has made significant legal advancements to address cybercrime. The evolution includes:

- Legislation Strengthening: Singapore enacted the Computer Misuse and Cybersecurity Act (CMCA) to address cyber threats comprehensively.
- National Cybercrime Action Plan: The government established the NCAP to coordinate efforts against cybercrime and enhance national cybersecurity.
- Adaptation to New Threats: Singapore's laws have evolved to deal with emerging tech-enabled threats, emphasizing legal tools alongside technological measures.

- Data Protection Enhancements: Developments in data protection laws, like the Personal Data Protection Act (PDPA), reflect the importance of safeguarding personal information.
- Strategy and Collaboration: The Singapore Cybersecurity Strategy highlights the government's commitment to addressing new and emerging cyber threats.

These changes demonstrate Singapore's proactive approach to adapting its legal framework to combat the evolving landscape of cybercrime and ensure robust cybersecurity." [4]

Which references the following:

1. law1.nus.edu.sg - An Overview of Cybercrime Legislation and Cases in ...
2. mha.gov.sg - National Cybercrime Action Plan (NCAP)
3. iclg.com - Cybersecurity Laws and Regulations Report 2023 Singapore
4. practiceforte.sg - Cyber law in Singapore: A Quick Overview (Part 1)
5. straitstimes.com - Singapore's laws need to evolve to deal with new tech- ...
6. fticonsulting.com - Singapore's Approach to Cyber Security
7. rsis.edu.sg - CYBER SECURITY IN SINGAPORE
8. csa.gov.sg - the-singapore-cybersecurity-strategy-2021.pdf
9. nortonrosefulbright.com - Singapore cybersecurity – new amendments introduce four key changes
10. thelawreviews.co.uk - The Privacy, Data Protection and Cybersecurity ... [4]

With regeneration of the results by ChatGPT, the following was obtained, from the same set of references:

"Over the last decade, Singapore has undergone significant legal changes to tackle cybercrime. The Computer Misuse Act (CMA) has been updated multiple times to cover new cyber threats and offenses. The National Cybercrime Action Plan was launched, emphasizing collaboration between public and private sectors.

Amendments to cybersecurity laws introduced key changes, including broader powers for law enforcement and enhanced penalties for cyber offenses. Singapore's cybersecurity strategy, like the Singapore Cybersecurity Strategy 2021, has been refreshed to address evolving threats.

Legal developments align with the rapid expansion of the digital landscape. The government emphasizes not only technological solutions but also legal tools to combat cybercriminal activities. These measures reflect Singapore's commitment to keeping pace with digital advancements and maintaining a secure cyberspace environment." [4]

The first answer to the second question by ChatGPT is shown below, with references to it.

"Over the last decade, technology in Singapore has advanced significantly to counter cybercrime:

Cybersecurity Strategy: Singapore's Cybersecurity Strategy 2021 emphasizes digital technology's role in improving lives while ensuring cybersecurity as a necessity and digital enabler.

National Action Plan: The National Cybercrime Action Plan urges individuals and enterprises to adopt better cyber hygiene practices, reducing opportunities for cybercrimes.

Technology Transformation: Advancements in portable devices and technology have transformed lifestyles, requiring strengthened cybersecurity measures to counter evolving cyber threats.

Challenges and Responses: The surge in cybercrime necessitates technological responses and policy changes to address the increasing frequency and severity of cyber threats.

Business Risks: Businesses are urged to reduce cybersecurity risks through measures such as employee education, technology adoption, and defense against cyber-attacks.

Government Initiatives: Government leaders stress the need for technological solutions to combat cybercrime, with cybercrime becoming a predominant mode of crime, surpassing physical crime.

Future Trends: Ongoing research and analysis of cybercrime trends shape strategies to counter evolving cyber threats and maintain the security of digital ecosystems.

Singapore's proactive adoption of technology-driven solutions reflects its commitment to mitigating cybercrime's impact and ensuring a secure digital environment.” [5]

With the following references:

1. csa.gov.sg - the-singapore-cybersecurity-strategy-2021.pdf
2. mha.gov.sg - National Cybercrime Action Plan (NCAP)
3. rsis.edu.sg - CYBER SECURITY IN SINGAPORE
4. dr.ntu.edu.sg - Strengthening cybersecurity in Singapore : challenges ...
5. roberthalf.com.sg - 5 ways to reduce cyber-security risks for businesses
6. htx.gov.sg - [SPEECH] SM Teo Chee Hean at TechX Summit
7. trendmicro.com - Cybercrime: Today and the Future [5]

Upon regeneration, the following was obtained using the same references.

“Over the last 10 years, technology in Singapore has seen significant evolution to mitigate cybercrime:

Cybersecurity Strategy: Singapore has formulated the Cybersecurity Strategy 2021, leveraging digital technology to enhance security against cyber threats and ensuring cyber hygiene practices.

National Action Plan: The National Cybercrime Action Plan emphasizes adopting better cyber hygiene practices to reduce opportunities for cybercriminals.

Advancements in Portable Devices: Rapid advancement in portable devices has transformed daily life, yet necessitates enhanced cybersecurity measures.

Business Risk Reduction: Organizations adopt measures such as the 5 ways to reduce cyber-security risks for businesses to safeguard against cyber-attacks.

Government Acknowledgment: Singapore's Deputy Prime Minister, SM Teo Chee Hean, noted that cybercrime has become a predominant mode of crime, motivating increased technological defenses.

These efforts collectively showcase Singapore's commitment to leveraging technological advancements to combat cybercrime and enhance cybersecurity across various sectors." [5]

The first answer to the third question by ChatGPT is shown below, with references to it.

"Over the last decade, Singapore has been actively working on promoting social norms and behaviors to discourage cybercrime:

Promoting Norms in Cyberspace: Internationally, Singapore recognizes the importance of promoting "norms" in cyberspace to deter cyber attackers and build trust.

Voluntary Non-Binding Norms: The Singapore Cybersecurity Strategy 2021 emphasizes the development and implementation of voluntary, non-binding norms that align with international law, aiming to establish responsible behavior in the digital realm.

These initiatives indicate Singapore's dedication to shaping positive social norms, fostering responsible behavior, and deterring cybercriminal activities through collaborative efforts at both national and international levels." [6]

The following were references cited.

1. rsis.edu.sg - CYBER SECURITY IN SINGAPORE
2. csa.gov.sg - the-singapore-cybersecurity-strategy-2021.pdf [6]

Upon regeneration, the same references were cited with the following answer.

"Over the past decade, Singapore has focused on evolving social norms to deter cybercrime:

Promoting Norms: Internationally, Singapore has taken steps to promote cyber norms as a deterrent, enhancing trust and security in cyberspace.

Cybersecurity Strategy: Singapore's Cybersecurity Strategy 2021 emphasizes advancing the development of voluntary, non-binding norms alongside international law.

These efforts are aligned with Singapore's aim to shape a secure digital landscape by fostering responsible behavior and advocating international norms to discourage cybercriminal activities." [6]

The first answer to the fourth question by ChatGPT is shown below, with references to it.

"Over the last decade, Singapore has experienced the following market-related developments to discourage cybercrime:

National Cybercrime Action Plan (NCAP): The government has established strategies focused on prevention as a key principle. This includes raising awareness and promoting preventive measures against cybercrime.

Increasing Cyberattacks and Response: Singapore has seen a significant increase in cyberattacks, prompting the need for robust cybersecurity measures. The market forces have driven the urgency to strengthen cybersecurity infrastructure.

Cybersecurity Strategy: The Singapore Cybersecurity Strategy 2021 emphasizes adapting to changing technological and strategic environments. The review and refresh of the cybersecurity strategy show a commitment to addressing cyber threats through market-driven solutions.

These developments reflect Singapore's efforts to align market forces with cybersecurity strategies, aiming to create a resilient digital environment and deter cybercriminal activities." [7]

With the following references:

1. mha.gov.sg - National Cybercrime Action Plan (NCAP)
2. trade.gov - Singapore Cybersecurity Market
3. csa.gov.sg - the-singapore-cybersecurity-strategy-2021.pdf [7]

And upon regeneration, the following surfaced.

"Over the last decade, Singapore's market forces have evolved to counter cybercrime through several strategies:

National Cybercrime Action Plan (NCAP): The government introduced the NCAP with principles focused on prevention, collaboration, and deterrence to ensure a safe online environment.

Cybersecurity Industry Growth: The Singaporean cybersecurity market has expanded, driven by increased cyber threats. This growth reflects the private sector's response to the rising demand for cybersecurity solutions.

Cybersecurity Strategy: The Cybersecurity Strategy 2021 outlines how Singapore will adapt to a changing strategic and technological environment by reviewing and refreshing its cybersecurity approach.

Public Awareness: Annual Scams and Cybercrime Briefs released by the police contribute to raising public awareness about cyber threats and encouraging individuals and businesses to adopt better cybersecurity practices.

These market-driven efforts demonstrate Singapore's commitment to leveraging market forces to combat cybercrime and enhance the nation's digital resilience." [7]

The following are the resources referenced.

1. mha.gov.sg - National Cybercrime Action Plan (NCAP)
2. rsis.edu.sg - CYBER SECURITY IN SINGAPORE
3. trade.gov - Singapore Cybersecurity Market
4. csa.gov.sg - the-singapore-cybersecurity-strategy-2021.pdf
5. dr.ntu.edu.sg - Strengthening Cybersecurity in Singapore
6. police.gov.sg - Annual Scams and Cybercrime Brief 2022
7. ink.library.smu.edu.sg - Cybercrime deterrence and international legislation
8. southeast-asia.kearney.com - Cybersecurity in ASEAN: An Urgent Call to Action [7]

4 Discussion

Firstly, it is clear that specific to Singapore's regulation of cybercrime, it has progressed significantly in its efforts to alleviate cybercrime. It does so in all aspects of Lessigs modalities. However, in the area of market forces, it does not appear that it was well distinct from the other modalities of constraints, which alludes to the second point for discussion.

Secondly, it does not appear that Lessigs modalities of constraints was adopted as a framework to explore Singapore's regulation of cybercrime over the last 10 years.

Many of the references relied on by ChatGPT were the one written 10 years ago. A cursory search on the usage of Lessigs in other countries revealed this by ChatGPT:
"One example of Lessig's modalities of constraints used in exploring the regulation of cybercrime beyond Singapore is found in the analysis of cybercrime regulation in various jurisdictions. Lessig's framework, including norms, law, architecture, and the market, has been applied to examine how different countries approach cybercrime regulation. For instance, researchers have evaluated how norms and laws vary in different legal systems, how technical architectures are designed to prevent cybercrimes, and how market incentives influence behavior and cybersecurity measures. This approach offers a versatile tool to understand the multifaceted nature of cybercrime regulation across different regions and legal contexts." [8]. With the following references:

1. cybercrimejournal.com - An Analysis of Regulation based on Lessig's four ...
2. researchgate.net - Cyber crime in Singapore: An analysis of regulation ...
3. academia.edu - Cyber Crime in Singapore: An Analysis of Regulation ...
4. erudit.org - Harms Of Loot Boxes And Approaching Regulation In ...
5. wikijuris.net - How is the Internet Regulated?
6. slideshare.net - Singapore's regulation of cybercrime
7. juscorpus.com - Unveiling the Shadows: Exploring Cyber Criminology and ...
8. journals.sfu.ca - Harms Of Loot Boxes and Approaching Regulation In ...
9. mha.gov.sg - JOURNAL
10. books.google.com.sg - Juvenile Delinquency: Theory, Practice, and Law [8]

Again, underscoring the fact that the framework is not commonly used.

Thirdly and more importantly, the preliminary study hints at technology being the most effective modality of constraints based on the responses given by ChatGPT as well as the citations found.

However, there are limitations to this study as it has not exhaustively tested out ChatGPT. It may have limited knowledge, as the information is based on its pre-trained data and might lack the most recent updates or specialized knowledge that's outside its training scope [9]. Moreover, its training scope does not include real-time information from the internet [9]. At times, it is known to spew inaccurate or misleading information, and as such, this paper sought to circumvent this issue by citing the references associated with each search.

Cybercrime's description is not clearly conceptualised in this paper, and may come across as broad. And it is very likely the case that certain modalities work better and/or more effectively on certain types of cybercrime. For example, technological measures would work better for hacking type of crimes, where as social norms and/or law may work for effectively for social engineering type of cybercrime. Future studies would do well to explore this further.

References

1. OpenAI. (2023, 7 August). Use of AI for Cybercrime. ChatGPT [3.5]. www.chat.openai.com
2. OpenAI. (2023, 25 August). Discuss Singapore's regulation of cybercrime based on Lawrence Lessig's modalities of constraints. ChatGPT [3.5]. www.chat.openai.com

3. OpenAI. (2023, 25 August). Discuss how Singapore’s regulation of cybercrime has changed based on Lawrence Lessig’s modalities of constraints. ChatGPT [3.5]. www.chat.openai.com
4. OpenAI. (2023, 25 August). Discuss how Singapore laws have evolved, over the last 10 years, to handle cybercrime. ChatGPT [3.5]. www.chat.openai.com
5. OpenAI. (2023, 25 August). Discuss how technology in Singapore have evolved over the last 10 years, to alleviate cybercrime. ChatGPT [3.5]. www.chat.openai.com
6. OpenAI. (2023, 25 August). Discuss how social norms in Singapore have evolved over the last 10 years, to discourage cybercrime. ChatGPT [3.5]. www.chat.openai.com
7. OpenAI. (2023, 25 August). Discuss how market forces in Singapore have evolved over the last 10 years, to discourage cybercrime. ChatGPT [3.5]. www.chat.openai.com
8. OpenAI. (2023, 25 August). Example of Lessigs modalities of constraints used in exploring regulation of cybercrime other than in Singapore. ChatGPT [3.5]. www.chat.openai.com
9. OpenAI. (2023, 26 August). Describe what ChatGPT is and its limitations. ChatGPT [3.5]. www.chat.openai.com

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.