



© Reuters

THAILAND'S CYBERSECURITY ACT:

*TOWARDS A HUMAN-CENTERED ACT
PROTECTING ONLINE FREEDOM AND PRIVACY,
WHILE TACKLING CYBER THREATS*



September 2019



MANUSHYA
Empowering Communities | Advancing Social Justice

Authors:

Emilie Palamy Pradichit,
Founder & Director
and

Ananya Ramani,
Human Rights Research & Advocacy Officer,
Manushya Foundation

.....

Publication design:

Laurene Cailloce,
Communications & Advocacy Volunteer,
Manushya Foundation

.....

Photos credit:

Cover page: Photo by Reuters, from Daily Mail Online; and Cybersecurity picture
from pexels.com

Inside cover: Picture from Mailfence

.....



This work is licensed under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License ("Public License"). To view a copy of this license, visit:
<https://creativecommons.org/licenses/by-nc-d/4.0/legalcode>

.....

Copyright @ManushyaFoundation2019

.....

***For more information about Manushya Foundation's Digital Rights project,
please contact:***



Emilie Palamy Pradichit, Founder & Director
emilie@manushyafoundation.org



Ananya Ramani, Human Rights Research & Advocacy Officer
ananya@manushyafoundation.org

THAILAND'S CYBERSECURITY ACT:

*TOWARDS A HUMAN-CENTERED ACT
PROTECTING ONLINE FREEDOM AND PRIVACY,
WHILE TACKLING CYBER THREATS*



Manushya Foundation would like to sincerely thank the **Embassy of the Kingdom of Netherlands in Bangkok, Thailand, Access Now, Thai Netizen Network** and the **International Federation for Human Rights (FIDH)** for their kind support and partnership on its *'Thailand's Cybersecurity Act'* project.



Kingdom of the Netherlands



accessnow

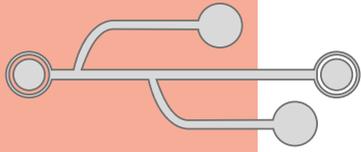


fidh

TABLE OF CONTENTS

Abbreviations	3
Acknowledgements	4
1. Introduction to Manushya Foundation's strategy to uphold digital rights and the project on the Cybersecurity Act	5
2. Background of the Study	7
3. Methodology	8
4. The Political and Legal Context & Framework of Thailand on the Digital Ecosystem	9
5. Challenges, Context & Recommended Amendments raised by Stakeholders regarding issues identified	13
5.1. Challenge 1: Broad scope and definition using <i>National Security, economic security, martial security and public order in the implementation and monitoring of the Act</i>	13
5.2. Challenge 2: Problematic substantive provisions and failure to define them in relation to <i>Three Level of Cyber Threats (non-critical, critical and crisis threats)</i>	18
5.3. Challenge 3: Controversial control mechanisms (government bodies and agencies) under the Act: <i>Top-down structure, broad powers given to authorities putting netizens under surveillance, lack of transparency and standards</i>	28
5.4. Challenge 4: Powerplay in the application of the Act: <i>Control over Critical Information Infrastructures (CIIs) and reporting obligations placed on them</i>	47
5.5. Challenge 5: Absence of checks and balances: <i>Cybersecurity Threats, lack of accountability and use of the Court system</i>	53
5.6. Challenge 6: Failure to ensure remedies: <i>Grievance redressal, imprisonment, fine and compensation</i>	56
6. Conclusion & Recommendations	61
ENDNOTES	64





ABBREVIATIONS

AIC	Asia Internet Coalition
APC	Association for Progressive Communications
ASEAN	Association of Southeast Asian Nations
BSA	Software Alliance
CCA	Computer Crimes Act
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CMO	Committee managing the Office of the National Cybersecurity Committee
CAN	Cyber Network Attacks
CRC	Cybersecurity Regulation Committee
CSO	Civil Society Organisation
EEF	Electronic Frontier Foundation
FCCT	Foreign Correspondents Club of Thailand
FIDH	International Federation for Human Rights
FOC	The Freedom Online Coalition
HDI	Human Development Index
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
ISP	Internet Service Providers
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
MDES	Ministry of Digital Economy and Society
MoJ	Ministry of Justice
MP	Member of Parliament
NBTC	Office of the National Broadcasting and Telecommunications Commission
NCPO	National Council for Peace and Order
NCSC	National Cybersecurity Committee
NHRCT	National Human Rights Commission of Thailand
NIA	National Intelligence Agency
NLA	National Legislative Assembly
NSC	National Security Council
RTG	Royal Thai Government
SEC	Securities and Exchanges Commission
TAG	Technical Advisory Group
UPR	Universal Periodic Review
UN	United Nations
UNDP	United Nations Development Programme

ACKNOWLEDGEMENTS



Manushya Foundation would like to sincerely thank everyone who contributed to the realisation of this study on ***Thailand's Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats***, particularly the Embassy of the Kingdom of Netherlands in Bangkok, Thailand, for its generous and steadfast support to develop this Study and in the organization of the Experts Meeting that was convened for the purpose of informing this Study; including H.E. Ambassador Kees Pieter Rade, Ambassador Extraordinary and Plenipotentiary; Kenza Tarqaat, Deputy Head of Economic and Political Affairs; and Thananart Chayanuch, Senior Political Officer. Manushya Foundation would also like to express its deepest appreciation for the guidance and support extended by all the co-organisers of the Experts Meeting, who have contributed to the organization of events related to this project such as the Experts Meeting, as well as the finalisation of this Study on challenges and amendments recommended to the Cybersecurity Act of Thailand; including the Thai Netizen Network, Access Now and the International Federation for Human Rights (FIDH). Special thanks are also extended to the Asia Internet Coalition (AIC) for their important input reflecting the private sector's perspective.

Manushya Foundation wishes to thank and express its deepest appreciation to all of the Experts that participated in the Experts Meeting to discuss Thailand's Cybersecurity Act that was held on 9 April 2019 and contributed to the content of the Study; particularly the Expert speakers and moderators at the event including Dr. Bhume Bhumiratana, Advisor to the National Cybersecurity Preparation Committee (Interim); Professor Emeritus Vitit Muntarbhorn, International Human Rights Law Expert and Professor Emeritus, Faculty of Law, Chulalongkorn University; Jeff Paine, Managing Director, Asia Internet Coalition (AIC); Sameer Sharma, Senior Advisor, International Telecommunications Union (ITU) Regional Office for Asia Pacific; Naman M. Aggarwal, Asia Pacific Policy Counsel, Access Now; Pavitra Ramanujam, Network Development Coordinator, Association for Progressive Communications (APC); Debbie Stothard, Secretary General, International Federation for Human Rights (FIDH); and Associate Professor Kanathip Thongraweewong, Digital Media Law Institution, Kasem Bundit University. Manushya Foundation also expresses its gratitude to all experts on digital rights, cybersecurity and information technology including Government advisors, the private sector, civil society, academic institutions, from the domestic, regional and international spheres for their time, effort and contributions to the knowledge on Thailand's Cybersecurity Act and at the Experts Meeting that contributed towards the development of this Study to serve as a guide not just in relation to amendments on the text of the Act to modify its content, but also on implementation and monitoring of the Act in the future.

Special thanks are also given to Manushya Foundation team members who developed this Study, by developing its framework, conducting desk research, analysis and writing, studying the international and national legal frameworks, analysis of these laws, incorporating challenges and expert opinions, towards the development of recommended amendments. These individuals are: Emilie Pradichit, Founder & Director and Ananya Ramani, Human Rights Research & Advocacy Officer. Manushya Foundation is also grateful to the following individuals for their research and design assistance Laurène Cailloce, Communications & Advocacy Volunteer; Evie van Uden, Human Rights & Development Researcher; and Silvia Fancello, Communications & Advocacy Intern.

Manushya Foundation would also like to sincerely thank those who made the launch of this Study possible including Mr. Andrea Giorgetta, Head of Asia Desk, FIDH on his organizational support; and Mr. Ramanjit Singh Chima, Asia Policy Director and Senior International Counsel and his organization Access Now for their financial support to the printing of the Study.

1. INTRODUCTION TO MANUSHYA FOUNDATION'S STRATEGY TO UPHOLD DIGITAL RIGHTS AND THE PROJECT ON THE CYBERSECURITY ACT

In its work, Manushya Foundation builds capacities on human rights monitoring mechanisms, sharing experiences, developing innovative strategies and strengthening solidarity; around various thematic areas of focus including Digital Rights. This is achieved by contributing to the promotion and protection of online freedom of expression and online privacy. To ensure local communities and local journalists are not subject to attempts to control the digital space, Manushya Foundation wishes to encourage governments to align their national legislation and policies with international standards. Similarly, Manushya would also like to lobby the private sector (particularly the ICT sector) to uphold digital rights and resist state pressure to control the internet. These are achieved through a strategy on Digital Rights with two objectives namely:

1. Upholding Digital Rights - online freedom and data privacy - by advocating for national legal frameworks and business activities to comply with international human rights standards;
2. Enhancing Digital Literacy & Safety by raising awareness and building the capacity of netizens to navigate the digital world safely.

In Thailand, in accordance with the first objective of upholding Digital Rights, Manushya Foundation is advocating for a National Cybersecurity Act which would respect online freedom and data privacy of Thai netizens, in line with international human rights standards, while effectively tackling cyberattacks and cybersecurity threats. For that purpose, Manushya Foundation in collaboration with the Embassy of the Kingdom of the Netherlands in Bangkok launched a project to study the National Cybersecurity Act of Thailand to ensure that it protects critical infrastructure from cyberattacks, while complying with international standards and upholding online freedom in the use of information and communication technology. Along with the Thai Netizen Network, Access Now, Association for Progressive Communications (APC), and the International Federation for Human Rights (FIDH), a multi-stakeholder Experts Meeting was organised on 9 April 2019 with perspectives from various experts including a government adviser; political party representatives; academics; private sector representatives; national, regional and international civil society organizations; a media representative; United Nations (UN) agency representatives; and diplomats. At the Experts Meeting, recommendations were provided on amendments, and improvements in relation to the implementation and monitoring of the National Cybersecurity Act in order for it to tackle cyberattacks, while complying with international standards on online freedom and data protection. Global good practices which could serve as a guide for this process were also discussed. With a comprehensive analysis of the finding from the Experts Meeting, a Study on ***“Thailand’s Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats”*** was developed as a guide to Thailand, its institutions, its private entities and its netizens, to contribute to a strong policy and streamlined process of implementation and monitoring of the National Cybersecurity Act in line with international human rights standards. This will be evaluated and discussed by national, regional, and international experts on cybersecurity, data privacy and communications infrastructure at the launch of the Study on Thailand’s Cybersecurity Act at the Foreign Correspondents Club of Thailand (FCCT) on 23 September 2019. This Study will be launched with the goal that it would be used as the basis to propose amendments to the National Cybersecurity Act of Thailand; and once implemented, the Act will continue to be monitored by a multi-stakeholder Technical Advisory Group (TAG).

DIGITAL LITERACY IN THAILAND PHASE I & PHASE 2

15 REGIONAL TRAINERS

DIRECTLY TRAINED

153 END-USERS



25 DIGITAL LITERACY TRAINERS

TRAIN

125 END-USERS

THE 278 END-USERS (THAI NETIZENS), ARE A PART OF A VARIETY OF DIFFERENT PROFESSIONAL BACKGROUNDS, INCLUDING:



STUDENTS



HUMAN RIGHTS DEFENDERS



ACADEMICS



JOURNALISTS



COMMUNITY MEMBERS



NGO WORKERS

MANUSHYA FOUNDATION STRATEGY



UPHOLDING DIGITAL RIGHTS:
TO CREATE A STRONG NETWORK OF THAI NETIZENS WHO ARE AWARE OF THE CYBER THREATS THEY MAY ENCOUNTER AND HOW TO EFFECTIVELY NAVIGATE A SECURE DIGITAL WORLD.

ENHANCING DIGITAL LITERACY:
FROM THIS, WE HOPE TO LAY THE GROUNDWORK FOR A SUSTAINABLE NETWORK, ABLE TO CONTINUE RAISING AWARENESS AND BUILDING CAPACITY OF DIGITAL LITERACY ACROSS THAILAND.

To realize its second objective, Manushya Foundation partnered with **Internews** on a Digital Literacy project, aimed at creating a network of Digital Literacy Trainers to increase the digital literacy of the broader Thai netizen community. During the workshops, the focus has been on three main areas, including knowledge on digital risks and threats, digital tools, and training ability. With the information and skills obtained through these workshops, and Manushya's ongoing mentoring and technical support, these Digital Literacy Trainers have been able to pass this knowledge to many other peers and members of their communities, with a focus on training journalists, human rights defenders and activists, and marginalized communities. All can now protect themselves against cyberattacks.

2. BACKGROUND OF THE STUDY

Cyberattacks or cyber network attacks (CNA) have been on the rise in Asia and in Thailand, with a constant increase in its threat ranking based on the cybersecurity risks it faces.¹ It was in these circumstances that the National Cybersecurity Act was developed in Thailand. While the purpose of the Act was met with support, it also faced strong opposition by civil society organizations (CSOs) and internet service providers (ISPs). Concerns were raised regarding the negative impact the Cybersecurity Act may have on Thai Netizens' right to freedom of expression online and respect to their privacy. While recognising the importance of tackling cybersecurity threats, Manushya Foundation believed it was important to create a safe space to discuss among relevant stakeholders the challenges the Cybersecurity Act may present and the opportunities available for the application of a human rights-based approach to cybersecurity, in order to guarantee cyberattacks are tackled while respecting the online freedom of Thai netizens. For that purpose, Manushya Foundation promoted a strong multi-stakeholder and human rights centred initiative to discuss policy challenges and key amendments, and to develop an independent implementation and monitoring mechanism from these collaborative efforts. With the government of the Netherlands placing Cybersecurity readiness and resilience at the forefront of its national agenda; they have strengthened their cybersecurity capability to address their internet infrastructure dependency and the vulnerabilities faced as a result. However, while building such capacity they have also ensured to continue promoting freedom of expression and internet freedom in their efforts. It is in this background that this project was conceived and launched by Manushya Foundation in collaboration with the Embassy of the Kingdom of the Netherlands in Bangkok.

This project analyses the text of the National Cybersecurity Act drafted by the Royal Thai Government (RTG). Through this project, focus was placed on guaranteeing that the Cybersecurity Act protects critical infrastructure from cybersecurity threats, while complying with international standards and upholding online freedom in the use of information and communication technology. Online freedom and privacy are specifically protected through international human rights standards and obligations, including United Nations (UN) human rights treaties, in particular the International Covenant on Civil and Political Rights (ICCPR) and UN recommendations generated through UN human rights monitoring mechanisms, such as the recommendations of the Universal Periodic Review (UPR) and through treaty body mechanisms specifically those of the human rights committee. Therefore, this project is also being implemented with a view to Manushya Foundation's thematic focus and its expertise on UN human rights mechanisms, whereby it empowers communities to meaningfully contribute to UN reporting and monitoring mechanisms. Furthermore, with Thailand as the 2019 chair of the Association of Southeast Asian Nations (ASEAN), it has set cybersecurity as one of the priorities for ASEAN this year. With this the RTG hopes to reinforce cybersecurity at the ASEAN level, by playing a major role in implementing measures to overcome cybersecurity threats within the region. This highlights the importance of the Cybersecurity Act and its implementation in Thailand, as it could see the replication of the Cybersecurity Act with its positive and negative provisions in all countries, at the ASEAN level.

This Study has been drafted with inputs received from the Experts Meeting on the Cybersecurity Act and it will serve as a comprehensive analysis on the findings of the meeting, with its recommendations for amendments serving as a guide to Thailand, its institutions, its private entities and its netizens, while contributing to a more streamlined process to the future implementation and monitoring of the National Cybersecurity Act in Thailand, in line with international human rights standards.

3. METHODOLOGY

CHALLENGES IDENTIFIED



CHALLENGE 1

Broad scope and definition

using National Security, economic security, martial security and public order in the implementation and monitoring of the Act

CHALLENGE 2

Problematic substantive provisions and failure to define them

in relation to Three Level of Cyber Threats (non-critical, critical and crisis threats)



CHALLENGE 3

Controversial control mechanisms (government bodies and agencies) under the Act

Top-down structure, broad powers given to authorities putting netizens under surveillance, lack of transparency and standards



CHALLENGE 4

Powerplay in the application of the Act

Control over Critical information infrastructures (CIIs) and reporting obligations placed on them



CHALLENGE 5

Absence of checks and balances

Cybersecurity Threats, lack of accountability and use of the Court system



CHALLENGE 6

Failure to ensure remedies

Grievance redressal, imprisonment, fine and compensation



The methodology used in the research, analysis, and drafting of this Study on the National Cybersecurity Act of Thailand included both primary and secondary sources. Primary sources that contributed to the knowledge in this document include information gathered from the Experts Meeting on the implementation of Thailand's Cybersecurity Act co-organized with the Embassy of the Kingdom of Netherlands in Bangkok, the Thai Netizen Network, Access Now, and FIDH on 9 April 2019, and through the contributions of Experts and participants at the meeting. This included challenges, amendments and recommendations identified and discussed during the event, with contributions received from various stakeholders and experts on digital rights, data protection, cybersecurity and critical infrastructure, including representatives from amongst government advisors, the private sector, civil society, academia, technical experts, national, regional, and international experts. These perspectives are divided based on the six main challenges identified, including: (1) **the broad scope and definition**, (2) **problematic substantive provisions and failure to define them**, (3) **controversial control mechanisms** (government bodies and agencies) under the Act, (4) **powerplay in the application of the Act**, (5) **absence of checks and balances**, and (6) **failure to ensure remedies**.

This Study and the amendments follow the unofficial translation by the government, as published on the website of the Ministry of Digital Economy & Society on 8 July 2019.² The Study was also informed by secondary sources through desk-research analysing the international obligations, regional commitments, national legal framework, gaps and challenges, expert opinions, international and regional best practices, and recommendations provided including those from UN human rights mechanisms and entities, government notifications, intergovernmental bodies, submissions by civil society, private sector viewpoints, multi-stakeholder policies, news articles, reports, studies, and conferences. All of this information, has also been compiled into a zero draft Study that was used to inform the Experts Meeting of 9 April 2019.

In this manner, this study aims at comprehensively evaluating the challenges that exist with respect to the text of the National Cybersecurity Act, providing a context for each of them, and proposing clear amendments to the text based on the international, regional and national laws and standards as well as best practices on digital rights and data privacy. In this manner, the Study provides an opportunity to identify textual amendments that can be used to serve as a guideline by members of parliament and political parties, to propose changes to the Act as adopted on 27 May 2019 in order to uphold international standards and regional commitments on online freedom and data privacy while tackling cybersecurity threats.

4. THE POLITICAL AND LEGAL CONTEXT & FRAMEWORK OF THAILAND ON THE DIGITAL ECOSYSTEM

POPULATION: 66.19 million³
HUMAN DEVELOPMENT INDEX (HDI): 0.755⁴
NUMBER OF INTERNET USERS IN THAILAND: 57 million⁵
LEVEL OF FREEDOM: 31/100 (with 0 being least free and 100 being most free)⁶
LEVEL OF PRESS FREEDOM: Ranked 140 of 180 countries⁷
LEVEL OF FREEDOM ON THE NET: 65/100⁸
RISK OF CYBERSECURITY THREATS: 18th in the world⁹
GLOBAL CYBERSECURITY COMMITMENT: 20 out of 164 countries (with 0 being highest and 164 being the lowest commitment)¹⁰

Following a military *coup* in 2014, the military suspended the Constitution and set up a National Council for Peace and Order (NCPO) through which the military continued to govern the country.¹¹ Although carried out with a claim to restore stability after a prolonged period of supposed political turmoil; it was accompanied with the partial suspension of the Constitution, the taking on of legislative powers,¹² and the use of the absolute authority of the NCPO to issue orders and make appointments without any oversight over the activities.¹³ This authority exercised resulted in the closing of the civic space with limits placed on assembly and association¹⁴ in the form of gatherings considered to be political, on freedom of speech and expression particularly any form of criticism and dissent,¹⁵ including through the use of *lèse-majesté* law.¹⁶

With respect to digital rights and online freedom, with a combination of cyber repression and social media manipulation, the tussle between politics and democracy continued both physically and online.¹⁷ Cyber repression is used in the form of restricting online content that is critical introducing a climate of fear and self-censorship, through the blocking or filtering of content on websites including under the Computer Crime Act (CCA).¹⁸ Individuals are also tried for these acts considered as cyber offences.¹⁹

After more than four years of military rule, Thailand held its first election on 24 March 2019, during which it suspended some of the orders that have an adverse impact on the rights of individuals including the right to political gatherings but new orders that will take effect with any legislative oversight were passed by the NCPO right till the elections.²⁰ Although having a record voter turnout,²¹ prior to the actual vote itself the political environment did not seem conducive to such an election with dissolution of the Thai Raksa Chart Party; charges against the leader and members of Future Forward Party under the CCA; and with the fairness of election laws, regulations and constitutional provisions coming into question.²² Also, unconfirmed reports of irregularities in voting came in from across the country, including with possible buying of votes in a number of provinces.²³ Without free and fair elections, there is little chance that the country will return to a true democracy. Additionally, with shrinking of civic space and silencing of dissent, an overall violation of rights will most likely continue unabated.

This can be understood better if an insight is provided into the domestic legal context and framework. The 2017 Constitution²⁴ in Article 32 establishes that everyone shall have the right to privacy, dignity, and reputation, with the abuse of personal information not being permitted unless provided by law and necessary for public interest.²⁵ The Constitution also provides under Articles 34 and 36 the rights to liberty, and freedom of expression and communication.²⁶ However, the liberty to express opinion can be restricted **‘for the purpose of maintaining the security of the State, protecting the rights or liberties of other persons, maintaining public order or good morals, or protecting the health of the people’**.²⁷ Section 36 also limits the liberty of communication by prohibiting censorship, detention or disclosure of information, except by a warrant issued by a Court where it is provided by law.²⁸ However, specific laws

are used to silence human rights defenders and dissidents voicing their concerns or undertaking their activities online.

The laws misused in this manner are as follows:

1. The Civil and Criminal Code of Thailand

Restrictions are placed on the freedom of expression through Sections 116 of the Criminal Code on sedition, Sections 326 and 328 of the Criminal Code,²⁹ and Section 423 of the Civil and Commercial Code on slander and libel³⁰ are examples of this, through their addressing of the crime of defamation in broadly-defined terms.

2. The Computer Crime Act (CCA)

While Thai law protects the access, interception and disclosure of communication in principle, it also provides certain exceptions by empowering government authorities under the regulatory framework of the Computer Crime Act of 2007³¹ governing information technology service providers, specifically with respect to incidents which are believed to have an effect on national security.³² The amendment to the Computer Crime Act³³ has raised concerns, as it allows the government unrestricted authority to limit free speech, conduct surveillance, and warrantless searches of personal data, as well as the ability to limit the freedoms to use encryption and anonymity.³⁴ It also holds service providers of the Information and Communications Technology (ICT) sector accountable for the actions of users.³⁵

3. The Personal Data Protection Act³⁶

At present, beyond the Constitution's provisions, Thailand does not have a general statutory law on data protection or privacy. The Personal Data Protection Act provides protection for personal data by restricting the collection, use, disclosure or tampering of personal data without the consent of its owner.³⁷ It also includes provisions with criminal penalties and civil liability.³⁸ The Act aims to regulate both data controllers and data processors, both within Thailand or outside of it that 'collect, use or disclose' the personal data of persons in Thailand regardless of their citizenship.³⁹ It includes general protections such as obtaining consent specifically from the subject whose information is being collected prior to or at the time of collection, either in writing or through electronic means. This consent may be revoked, unless there is restriction on such revocation. In addition, the collection of data must be for a lawful purpose and be of direct relevance or necessary for the activities of the data controller. However, the person must be informed by the data controller of the purpose of the data collection; the data to be collected; the person to whom the data will be disclosed; the contact details of the person whose data is controlled; and the rights that he/she is guaranteed. The collection of sensitive personal data such as the political preferences, the medical records or the religious beliefs of a person is prohibited, unless it is permitted under the draft Act or by a ministerial regulation.

The Act provides exceptions in the form of data collected to protect or prevent harm to a person's life, body or health, or for the compliance with a legal requirement. The subject whose information has been collected may request to access data that has been collected or to determine the source of the information, where the collection has been done without the consent of the person. Deletion, destruction or temporary suspension of the use or anonymising of personal data may be requested where the data controller fails to comply with the provisions of this Act; and such violations may be subject to civil and criminal penalties. With respect to privacy and Cybersecurity, the Personal Data Protection Act only refers to cybersecurity protection as a limitation to the protection of data privacy in Section 41/4 and suggests that the Personal Data Protection Committee provide advice or consult with government agencies and private sector organizations on any operations to ensure the protection of personal data under Section 16(9).⁴⁰ **However, this remains open to interpretation with no explanation on how cybersecurity operations that violate data privacy are addressed.**

Even in this political and legal climate, Cybersecurity is seen as an important issue as highlighted from the statistics above, due to the risk posed to Thailand by cybersecurity threats and cyberattacks, and the effect such cybersecurity threats and cyberattacks could have on the critical information infrastructure of the

country. This critical infrastructure, if affected, could damage vital systems and assets.⁴¹ To address this, it is essential that any State takes steps with respect to three factors including: (1) **creating a legislative and policy framework**; (2) **developing cyber capabilities and the technical capacity of individuals in the country**; and (3) **building the political will to implement such legislation or policy with respect for the other international commitments of the country**, including international human rights standards while tackling cybersecurity threats and cyberattacks; as will be analyzed below.

TIMELINE OF EVENTS IN THE DEVELOPMENT OF THE NATIONAL CYBERSECURITY ACT



1 6 JANUARY 2015
The first draft of Cybersecurity Act is approved in principle, by a Cabinet resolution.

24 MAY - 7 JUNE 2017
The Ministry of Digital Economy and Society organizes public hearings on the second draft of the Cybersecurity Act.



3 25 MARCH 2018
The Ministry of Digital Economy and Society publishes the latest draft of the Act for public hearing and public consultation.



27 SEPTEMBER-12 OCTOBER 2018
The third draft of the Cybersecurity Act is open for public consultation, following amendments made by the National Cybersecurity Preparation Committee.



5 OCTOBER 2018
The draft is approved by the Office of the Council of States.



31 OCTOBER 2018
A meeting is organized to receive comments and suggestions on the Cybersecurity Act from experts and representatives of the Technology Crime Suppression Division.



7 16-30 NOVEMBER 2018
A second public hearing is open for 15 days. The Ministry of Digital Economy and Society holds a trilateral committee meeting which is between the government sector, CSOs and the private sectors, in order to amend the draft.



13 27 MAY 2019
Following the approval and signature by the King, the Cybersecurity Act is published in the Royal Thai Government Gazette, by which it comes into effect.

26-28 FEBRUARY 2019
The NLA considers the Cybersecurity Act at its second and third reading. The Act is adopted by a unanimous vote of those present on 28 February.



11 18 FEBRUARY 2019
The NLA Ad hoc committee submits its report on the Cybersecurity Act to the NLA for the second reading.



27 DECEMBER 2018 - 17 FEBRUARY 2019
The NLA Ad hoc committee reviews the content of the Cybersecurity Act, prior to submission before the NLA for a second reading.



9 27 DECEMBER 2019
The NLA passes the Cybersecurity Act, in its first reading.



8 18 DECEMBER 2018
The Cabinet approves the Cybersecurity Act, submitting it to the National Legislative Assembly. The Act is approved with an amendment requiring a court warrant in cases where authorities want to access computer systems to obtain personal information.

5. CHALLENGES, CONTEXT & RECOMMENDED AMENDMENTS RAISED BY STAKEHOLDERS REGARDING ISSUES IDENTIFIED

5.1.

Challenge 1: Broad scope and definition using National Security, economic security, martial security and public order in the implementation and monitoring of the Act



5.1.1. Context

“The National Cybersecurity Act of Thailand is part of an already shrinking democratic space, and so the government must review this law and deal with it in a reasonable manner keeping in mind democratic aspirations.”

Professor Vitit Muntarbhorn,
International Human Rights Law Expert
and Professor Emeritus, Faculty of Law,
Chulalongkorn University

At the outset, the National Cybersecurity Act (*hereinafter referred to as Act*) has challenges in the scope of its application and the definition of various aspects under the legislation, which is a violation of international law, that requires drafting of legislations to be done in a clear and narrow manner and not leaving too much to interpretation. The jurisdiction of the Act focuses on security and particular versions of it, such as ‘national security, economic security, military security and public order’, without clarity on the definition and configurations of those security measures. This contravenes with article 19(3) of the International Covenant on Civil and Political Rights (ICCPR) and the International Principles on the Application of Human Rights to Communications Surveillance (13 Principles), which permit limitation to freedom of expression, as long as those restrictions are provided by law, necessary and proportionate.

The jurisdiction of the Act, and the terms used to define what the Act applies with respect to, how it is applied, who it is applied with respect to, and who enforces the Act are very broad and often do not take into consideration individual rights or international standards or human rights starting with the Preamble to the Act. The Preamble which sets the tone of the whole Act, broadly limits rights and freedoms of persons as provided for in the Constitution, without actually defining how far these limits will apply. Moreover, it states that the necessity to restrict rights is based on the need to protect, address and mitigate cybersecurity threats that affect national security and public order. National security or public order have not been defined, but it is often misused

to guarantee the security of the State and the interests of its government; and public order is misused in all situations where an individual from civil society does anything that could threaten the State ‘interests’.



Both these aspects could be used to prioritize this misunderstood idea of cybersecurity and take actions to tackle cybersecurity threats under the Act, without considering the effect it could have on Thai netizens and the general public. This does not clearly explain how these limitations will apply and be used. In this respect, any limitation should be clearly provided so that its use can be anticipated and it should be re-evaluated collectively with changes made according to developments with respect to technology and society. Moreover, to provide protection, it is essential that throughout the Act international standards and obligations that Thailand has committed to, are applied.

a. WHAT does the Act apply to? Maintaining Cybersecurity and its understanding

In Section 3, this Act addresses the security angle of Cybersecurity by primarily looking at its impact on the functions of the State, defining it as the risk posed to national security, economic security, martial security, and public order collectively. Therefore, Cybersecurity in this manner is seen to focus more on stability of the State, political security or maintaining political power, and less on protection of the constituents of the State from threats that are posed in the digital space.

While broad in its scope, three gaps can be found in the failure to properly define the scope of Cybersecurity under the Act:

- (1) The security of individuals and netizens is completely ignored;
- (2) National security, economic security, martial security, and public order are not defined which leaves it open to interpretation. It is of concern specifically in the case of 'national security' that has been misused and led to the violation of human rights of individuals. This can be resolved by including and using it collectively with the security of individuals, including protection of their rights as a priority;
- (3) There has been no explanation on how a cybersecurity risk actually affects and threatens the digital ecosystem. Therefore, the effect on information and information infrastructure, specifically their availability, confidentiality and integrity⁴² must be taken into consideration.

b. HOW the Act is applied? Methods of implementation

Ambiguity continues in the Act, as processes must follow different rules or regulations that are not clearly explained in the Act. For example, a code of practice developed by the Cybersecurity Regulation Committee (CRC) serves as guideline for the implementation of the Act by different authorities as identified by Sections 3, 13, 22, 44, 45, and 56. Under this, the CRC is given broad powers to draft this code in any manner that it would like to, without any explanation on substantive or procedural checks and balances to protect individual rights. Therefore, it would be important to place safeguards by limiting it in substance to that which is necessary⁴³ to achieve a legitimate aim and proportionate⁴⁴ to the threat that is being faced. Procedurally, the guidelines must also be limited to apply only to the use of computer assets, communication structures and networks that the CRC has authority over; as set out in the Act.

c. WHO does the Act apply to? Structures that are governed by the Act

To meet the goal of protection in cyberspace, information assets and associated infrastructure essential to support the State, must be protected. This infrastructure called Critical Information Infrastructure (CII) does not have a single, commonly accepted, universal definition. It must instead be defined based on a country's individual risk assessment that is based on the national context. However, Sections 3 and 49 of the Act provide an open-ended scope for identifying or designating CIIs. This results in four overall issues:

- (1) **Broad understanding of the link between infrastructure and the key aspects to be protected:** Identifying all computers or computer systems connected in any manner with national security, public order, economic security and public interest will allow for interpretation that could lead to misuse.

This is primarily because a link could be drawn between any infrastructure and the key aspects identified, which could result in all information infrastructures and their work being supervised or monitored. This can be resolved by narrowing the identifying of CIIs not just based on the link they have to a key aspect that must be protected, but by drawing a link between the damage to the organization and its resulting destructive impact on a vital aspect requiring protection.

- (2) **Excessive power given to government authorities, without input of other stakeholders:** The above identified broad linkage is specifically damaging because the categories of CIIs identified under Section 49 are broad without clear examples provided and are left open ended, with the NCSC given discretion to designate any other organization as a CII. In this way, CIIs could be restricted by strict control exercised over them by primarily government bodies and agencies, and this could be used to crush democratic aspirations by forcing compliance on organizations that could be doing work the government does not agree with or that it could see as a threat to its retention of power. This can be addressed by requiring clearly identifiable characteristics, receiving input from other stakeholders on the criteria, limiting control to situations that would be considered legitimate in a democratic society, and by allowing for review of such criteria by an independent multi-stakeholder body.
- (3) **Ignoring the impact on individuals' privacy:** The security and privacy of individuals from civil society and that of netizens continues to be ignored even in the identification of CIIs under the Act. Adding this to the Act will help resolve the gap this could cause.
- (4) **Separation of powers:** CIIs include both government agencies as well as private organizations. Government Agency have defined in Section 3 to include a whole range of government functionaries such as those that are part of the central government, regional government, local government, state enterprises, the legislative institution, the judicial institution, independent institutions, public agency, and other government agencies. With such a wide scope, there is a lot of opportunity for misuse, especially to gain control over the processes of judicial institutions or of legislative institutions.

d. WHO enforces the Act? Authorities responsible for implementation and monitoring

The Act sets up various bodies and agencies, assigning them roles and duties for the implementation of the Act, which are often broad and completely unregulated. Three challenges that exist with respect to this are: (a) *authorities being given very broad power as identified above with respect to the identification of CIIs*; (b) *the same authorities perform multiple functions under the act by supervising and then regulating these rules, such as in the case of supervising or regulating organizations as defined by Section 3*, and (c) *the absence of any independent monitoring of the power exercised by government authorities under this Act*, for which the establishment of a multi-stakeholder entity that handles complaints on unfair investigations, monitors and evaluates performance under this Act is recommended.

"With respect to the National Cybersecurity Act of Thailand, it has been discovered that only experts were part of the discussion on its drafting. Communities are not aware that they would be impacted if the Cybersecurity Act does not follow international standards. Building their capacity, including their contribution to the implementation and monitoring of the Act along with other stakeholders is the only way forward."

Emilie Pradichit,
Founder & Director, Manushya Foundation

5.1.2. Recommended Amendments

Original Text (in sequential order)	Suggested Changes, Deletions and Additions to the National Cybersecurity Act
<p><i>Preamble:</i> This Act contains certain provisions in relation to the restriction of rights and freedoms of persons, which section 26 in conjunction with Section 28, Section 32, Section 32, Section 34, Section 36, and Section 37 of the Constitution of the Kingdom of Thailand so permit by virtue of the law.</p> <p>The rationale and necessity to restrict the rights and freedom of a person in accordance with this Act are to efficiently protect cybersecurity and to establish approaches to protect, cope with, and mitigate the risk of cyber threats which affect the national security and public order. The enactment of this Act is consistent with the criteria prescribed under section 26 of the Kingdom of Thailand.</p>	<p><i>Preamble:</i> This Act contains certain provisions in relation to the restriction of rights and freedoms of persons, which section 26 in conjunction with Section 28, Section 32, Section 32, Section 34, Section 36, and Section 37 of the Constitution of the Kingdom of Thailand so permit by virtue of the law, and subject to international standards and obligations applicable to the Kingdom of Thailand, both online and offline while having to respect human rights and technological innovation.</p> <p>The rationale and necessity to restrict the rights and freedom of a person in accordance with this Act are to efficiently protect cybersecurity and to establish approaches to protect, cope with address, and mitigate the risk of cyber threats which affect the national security and public order. The enactment of this Act is consistent with the criteria prescribed under section 26 of the Kingdom of Thailand.</p> <p>However, this Act shall only limit rights and freedoms through standards that are clear and precise in order to foresee the application of the law in advance, with periodic review of these limitations through a collective and participatory process.</p>
<p><i>Section 3:</i> In this Act “Maintaining Cybersecurity” shall mean any measure or procedure established to prevent, cope with, and mitigate the risk of cyber threats from both inside and outside the country which affect national security, economic security, martial security, and public order.</p>	<p><i>Section 3:</i> In this Act “Maintaining Cybersecurity” shall mean any measure or procedure established to prevent, cope with address, and mitigate the risk of cyber threats from both inside and outside the country which affect the availability, confidentiality and integrity of information and its infrastructure that threaten national security, economic security, martial security, and public order and security of persons.</p>
<p><i>Section 3:</i> “Government Agency” shall mean the central government, regional government, local government, state enterprises, the legislative institution, the judicial institution, independent institutions, public agency, and other government agencies</p>	<p><i>Section 3:</i> “Government Agency” shall mean the central government, regional government, local government, state enterprises, the legislative institution, the judicial institution, independent institutions, public agency, and other government agencies, with due respect to the independence of these institutions and the separation of powers that the government is subject to.</p>
<p><i>Section 3:</i> “Code of Practice” shall mean any regulations or rules determined by the Cybersecurity Regulation Committee.</p>	<p><i>Section 3:</i> “Code of Practice” shall mean any regulations or rules determined by the Cybersecurity Regulation Committee, which shall be necessary and proportionate, to establish the correct use of computer assets, networks and electronic communication of concerned structures under the authority.</p>

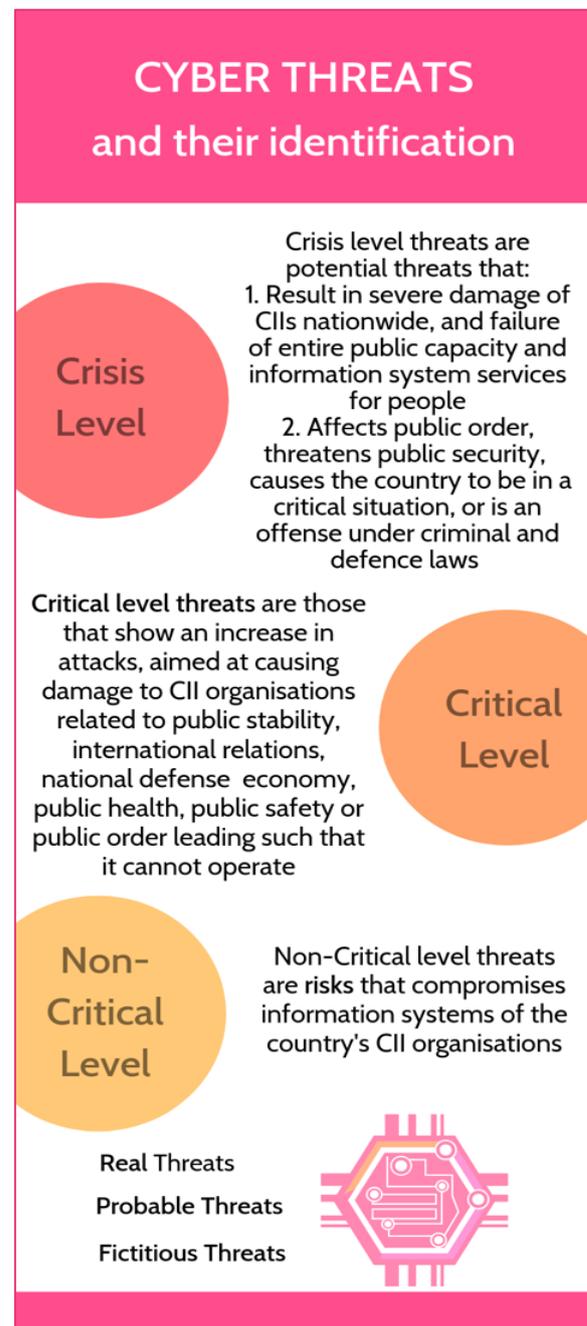
<p><i>Section 3: “Critical Information Infrastructure” shall mean the computer or computer system that the Government Agency or private organization uses in their operations which relate to maintaining national security, public security, national economic security, or infrastructures in the public interest.</i></p>	<p><i>Section 3: “Critical Information Infrastructure” shall mean the computer or computer system that the Government Agency or private organization uses in their operations, which relate to the destruction of which will have a damaging effect on maintaining national security, public security, national economic security, individuals’ security and privacy, or infrastructures in the public interest in a manner that is legitimate in a democratic society.</i></p>
<p><i>Section 3: “Supervising or Regulating Organization” shall mean a Government Agency or private organization or a person that is appointed by law to have the duty and power to supervise or regulate the operations of a Government Agency or Organization of Critical Information Infrastructure</i></p>	<p><i>Section 3: “Supervising or Regulating Organization” shall mean a Government Agency or private organization or a person that is appointed by law to have the duty and power to supervise or regulate the operations of a Government Agency or Organization of Critical Information Infrastructure. Supervision of the implementation of this Act, and regulation of such activity shall not be carried out by the same, body, authority or organization.</i></p>
	<p><i>Section 3: “Tripartite Agency” means an independent entity consisting of competent individuals representing different stakeholder groups such as the government, the private sector, technical experts, Civil Society Organizations (CSOs), netizens, and the National Human Rights Commission of Thailand (NHRCT); established to ensure accountability through monitoring and evaluation of the clauses of the work of the NCSC, the CRC, and the NCRA under the Act. The tripartite agency shall also have the power to review and handle complaints as well as unfair investigation procedures that have occurred under the Act.</i></p>



5.2.1. Context

In order to be able to respond to cybersecurity incidents or threats faced in cyberspace, the first step taken is the identification of vulnerabilities and the threats that could arise. This is the basis for the substantive provisions under the National Cybersecurity Act, which recognizes three types of cybersecurity threats, namely **non-critical**, **critical**, and **crisis level** cybersecurity threats under Section 60. These threats are identified based on the likelihood of their occurrence and their potential impact on CIIs, as set out in the corresponding infographic.

In analytical terms, the likelihood of the occurrence of a cybersecurity threat can be divided into three notions or understanding of the threat. These can be both offensive and defensive, so that an incident can be pre-empted before it can cause harm to a country and its infrastructure. These include **real threats** or those that can be proved; **probable threats** or those that may be a threat; and **fictitious threats**. To explain, in the case of a crisis level cyber threat, it is almost always the existence of a possible threat or one that may arise which is identified to determine its existence. In the case of a critical level cyber threat, a more real threat has to be identified as it requires both the aim being to attack or the existence of intent; and a clear impact in the form of damage caused to the essential infrastructure of CII organizations and their corresponding failure to operate or provide services. A fictitious threat could also be used to identify all the three types of cybersecurity threats whether non-critical, critical or crisis level since the power to define a cybersecurity threat level is given to the NCSC. **As a result, the NCSC that defines what would amount to the existence of a real, possible or a fictitious threat will have the power to 'make' a threat, even where one does not exist.** The only method to prevent such misuse when it comes to substantive provisions would be by defining limits and conditions as identified below in the identification of cybersecurity threats, in the assessment of damage caused and in determining responses once they have been identified.



a. Protection of the rights of individuals

“Cybersecurity legislations often use manipulation by offering citizens protection against cybersecurity threats in exchange for freedom of speech, thus compromising on citizens’ rights. Instead, cybersecurity legislations should aim to protect individuals, who are the ultimate victims of all cyber threats.”

Pavitra Ramanujam,
Network Development Coordinator,
Association for Progressive
Communications (APC)

In an attempt to protect against cybersecurity threats, the rights and protections guaranteed to individuals should not be done away with. Therefore, in the assessment of damage caused by a cybersecurity threat under Section 58 as well as in the identification of cybersecurity threats under Section 60 particularly at the crisis level; human rights as enshrined in the Constitution, in this Act as well as other related domestic and international legislations must be protected. For this, no action must be taken that is in conflict with rights as identified in these legislations. Further, rights must also be protected in all action taken by the Cybersecurity Regulation Committee (CRC) and as supervised by the NCSC in preventing, addressing, mitigating threats, and providing damages under Sections 64 and 65 of the Act respectively.

The right to privacy must be specifically guaranteed under Section 65 and 66 of the Act that are related to providing damages caused by a threat and in taking steps to prevent, address or mitigate critical level threats respectively. In the case of critical level threats, such protection of privacy must be guaranteed in the case where computer systems or computers are accessed with officials extracting and maintaining a copy of the information extracted. Here an attempt must be made to notify persons who could be affected by this information gathering, and restrictions must be placed on the handling of the information to safeguard all personal information. Failure to do this could result in the information collected being misused to try individuals based on the content of the information, under other laws. This has been restricted by collecting and retaining information ‘as necessary’ in some sections of the Act, but this is not uniform and whether this aspect translates in practice has to be seen. Additionally, data protection must be guaranteed throughout the Act with the Committee managing the Office of the National Cybersecurity Committee (CMO) specifically responsible for data protection of collected data and information.

b. Protection of affected systems

To protect systems that have been affected by cybersecurity threats from further damage that could result while preventing, addressing or mitigating a threat, safeguards must be guaranteed for information and information systems. This can be done by preventing damage to the availability, confidentiality and integrity⁴⁵ of information and information systems under Section 58 on assessment of damage, Section 60 on defining the cybersecurity threats, and Section 65 related to providing damages caused by a threat under the Act.

c. Higher standard of proof

The standard of proof set in the Act, particularly with respect to critical and crisis level cybersecurity incidents is very **problematic** for two reasons:

- (1) **Basing the identification of a threat on suspicion it presupposes guilt even before investigation.**⁴⁶
Under Section 66 in responding to critical level cybersecurity incidents, the CRC can order officials to seize or freeze computers, computer systems or equipment that is related to the cybersecurity threat,

for examination and analysis investigate the premises with the permission of the owner based on suspicion and the NCSC can also request the court to pass orders to officials stating that a suspicious act or person could cause a critical level threat. **The standard of proof instead of ‘reason to suspect’ should instead be the existence of ‘evidence to believe’.**⁴⁷

- (2) **‘Possible’ threats do not have an actual set standard of proof to determine the possibility of the existence of a threat:** as addressed in Sections 58 to 66, possible threats have not been defined or explained throughout the Act. Therefore, it would be appropriate in this case to identify the seriousness of it by using the standard of **‘where there is evidence to believe that there may be a risk of serious harm.’**

d. Precautions to be taken while identifying cybersecurity threats

In addition to listing the types of cybersecurity threats to the digital ecosystem, the Act must also define the clear responsibilities and tasks of entities responsible for identifying and collecting information on vulnerabilities. This remains incomplete as assessing and evaluating vulnerabilities for potential threats as provided in Section 62, has left out some important aspects, including that: (a) identification must be strictly in accordance with criteria set out by this Act; (b) such criteria must be made publicly available; and (c) any identification must be supported by evidence.

e. Precautions to be taken while responding to cybersecurity threats

In response to the existence and the recognition of a cybersecurity threat, the various bodies and entities under the Act have been assigned various tasks and responsibilities. However, all the tasks have not been clearly outlined leading to several gaps, as found in Sections 63, 64, 65, and 66 on responding to these cybersecurity threats. They can be addressed with the following additions:

- (1) Any response with respect to cybersecurity threats must be as necessary to prevent, address and mitigate the threat, proportionate to the extent required, and must include appropriate action;
- (2) Permission obtained from an owner to enter, access, and search premises must be voluntarily given prior to the action taken to analyse and evaluate the effects from cybersecurity threats;
- (3) Monitoring computers and computer systems must be limited to the period for or with reason to believe that a threat exists;
- (4) When checking computers or computer systems to identify any problems that could block cybersecurity, the situation should be analysed and the impact assessed with due care and in a timely manner;
- (5) Confiscating computers or computer systems in the case of crisis level cybersecurity incidents must only take place following a clear explanation of the evidence available to establish such belief;
- (6) While responding to a cybersecurity incident, damage to officials must be avoided to the extent possible and only in circumstances where it cannot be avoided should the damages incurred be reimbursed;
- (7) The code of practice of the CRC with rules and regulations to be followed as a guideline in maintaining cybersecurity, must be publicly available and accessible; and
- (8) Reports on progress shall be submitted to the CRC once the threats have ceased and these shall be made available to the general public including information on evaluating and determining the existence of cybersecurity incidents.

f. Provision of remedy

“In the Thai context, there is a lack of public trust as laws are often misused. The National Cybersecurity Act also has the potential to negatively affect human rights and the private sector, because it does not provide certainty. This is more difficult as the Act does not include a monitoring device. Therefore, it is questionable how consistency can be reached when the Act is enforced.”

Debbie Stothard,
Secretary General, International Federation for Human Rights (FIDH)



To balance the needs of the State to protect against cybersecurity risks with those of individuals, procedural safeguards must be integrated in the form of effective oversight and remedies. Access to the court system is only permitted for non-critical and critical cybersecurity incidents, with the Act only providing for reporting to the Court after a crisis level cybersecurity incident has already been addressed.

Therefore, the Act must allow for court permission and oversight in cases of crisis level threats. First, the Act must guarantee that court permission would be sought to identify crisis cybersecurity threats supported by evidence to believe that there may be a risk of serious harm. Second, the Act must ensure that an independent multi-stakeholder tripartite agency will determine the appropriateness of action taken, its extent, the resulting damages, and the reimbursement provided.

Further, remedy must be permitted against the authorities established under this Act for the misuse, wrongful application or excessive action taken by them in such circumstances including in the form of temporary orders and injunctions, which can be determined by any effective grievance redressal mechanism. A special Court may be established for this purpose, which could include specialized judges who obtain necessary legal and technical expertise, as well as the knowledge of the content and processes of the Act in order to consider cases in relation to it. This could also be undertaken through an ombudsperson.

5.2.2. Recommended Amendments

Original Text (in sequential order)	Suggested Changes , Deletions and Additions to the National Cybersecurity Act
<p><i>Section 58:</i> In the case there is or may be a Cyber Threat to an information system that is under the responsibility of a Government Agency or an Organization of Critical Information Infrastructure, such organization shall examine its related information, computer data, and the computer</p>	<p><i>Section 58:</i> In the case there is or may be a Cyber Threat to an information system that is under the responsibility of a Government Agency or an Organization of Critical Information Infrastructure, such organization shall examine its related information, computer data, and the computer</p>

<p>system, including the surrounding circumstances to assess whether a Cyber Threat has occurred. If the examination results show that there is or may be a Cyber Threat, the organization shall prevent, cope with, and mitigate the risks from such Cyber Threat in accordance with the Code of Practice and standard framework in Maintaining Cybersecurity and shall notify the Office and its Supervising or Regulating Organization without delay.</p>	<p>system, including the surrounding circumstances to assess whether a Cyber Threat has occurred in situations where there is evidence to believe that there may be a risk of serious harm. If the examination results show that there is or may be a Cyber Threat, the organization shall prevent, cope with address, and mitigate the risks from such Cyber Threat in accordance with the Code of Practice and standard framework in Maintaining Cybersecurity and shall notify the Office and its Supervising or Regulating Organization without delay in a manner that does not compromise the integrity of the system and rights of individuals.</p>
<p><i>Section 59:</i> When it appears to the Supervising or Regulating Organization, or when the Supervising or Regulating Organization is notified of an incident in accordance with section 58, the Supervising or Regulating Organizations in cooperation with the organization under Section 50 shall gather information, examine, analyse the situation, and evaluate the effects related to the Cyber Threat and shall perform the following</p>	<p><i>Section 59:</i> When it appears to the Supervising or Regulating Organization, or when the Supervising or Regulating Organization is notified of an incident in accordance with section 58, the Supervising or Regulating Organizations in cooperation with the organization under Section 50 shall gather information, examine, analyse the situation, and evaluate the effects related to the Cyber Threat and in situations where there is evidence to believe that there may be a risk of serious harm shall perform the following</p>
<p><i>Section 60:</i> In considering to exercise power to prevent Cyber Threats, the Committee will determine the type of Cyber Threat as classed into three levels, as follows:</p> <ol style="list-style-type: none"> (1) a Cyber Threat at non-critical level means a Cyber Threat with significant risk at a level which causes the computer system of the country's Organization of Critical Information Infrastructure to be compromised; (2) a Cyber Threat at a critical level means a Cyber Threat with the nature of having significant increase in computer system, computer or computer data attacks, with the aim to attack the Organization of Critical Information Infrastructure of the country, and such attack has the effect of causing damage to the computer system of the information technology infrastructure related to the operation of the Organization of Critical Information Infrastructure of the country, public stability, international relations, national defense, economy, public health, public safety, or the public order, such that it could not operate or provide service; (3) a Cyber Threat at a crisis level means a Cyber Threat in a crisis level of the following nature: <ol style="list-style-type: none"> (a) is a Cyber Threat occurring from a computer system, computer, computer data attacks in a level higher than the Cyber Threats in a critical level, which cause severe effect to Critical Information Infrastructure of the country in a large-scale and which causes the whole operation of Government Agency or the provision of service of Organization of Critical Information 	<p><i>Section 60:</i> In considering to exercise power to prevent Cyber Threats, the Committee will determine the type of Cyber Threat as classed into three levels, as follows:</p> <ol style="list-style-type: none"> (1) a Cyber Threat at non-critical level means a Cyber Threat with significant risk at a level which causes the computer system of the country's Organization of Critical Information Infrastructure to be compromised by impairing the availability, confidentiality and integrity of information and information systems; (2) a Cyber Threat at a critical level means a Cyber Threat with the nature of having significant increase in computer system, computer or computer data attacks, with the aim to attack the Organization of Critical Information Infrastructure of the country, and such attack has the effect of causing damage and affect the availability, confidentiality and integrity of information and that of to the computer system of the information technology infrastructure related to the operation of the Organization of Critical Information Infrastructure of the country, privacy, public stability, international relations, national defense, economy, public health, public safety, or the public order, such that it could not operate or provide service; (3) a Cyber Threat at a crisis level means a Cyber Threat in a crisis level owing to situations where there is evidence to believe that there may be a risk of serious harm of the following nature:

<p>Infrastructure to fail, such that the state could not control the operation center of the state's computer system, or the normal remedial measures for Cyber Threat could not resolve the issue and there is risk of spreading to other critical infrastructure of the country, which may cause death to many people or cause a great amount of computer system, computer, and computer data to be destroyed in a large-scale on a national level;</p> <p>(b) is a Cyber Threat that affects or may affect the public order or is a threat to public security or may cause the country or part of the country to be in a critical situation, or an offense regarding terrorism under the Penal Code, battling or war, which an urgent measure is required to maintain the democratic form of government with the King as the Head of the State in accordance with the Constitution of the Kingdom of Thailand, sovereignty and the integrity of the territory, national benefit, compliance with the laws, public safety, normal living of the public, protection of freedom and rights, public order or benefit, or the protection or remedy of damages from the public disaster that is emergency and critical.</p>	<p>(a) is a Cyber Threat occurring from a computer system, computer, computer data attacks in a level higher than the Cyber Threats in a critical level, which cause severe effect to Critical Information Infrastructure of the country in a large-scale and which causes the whole operation of Government Agency or the provision of service of Organization of Critical Information Infrastructure to fail, such that the state could not control the operation center of the state's computer system, or the normal remedial measures for Cyber Threat could not resolve the issue and there is risk of spreading to other critical infrastructure of the country, which may cause death to many people or cause a great amount of computer system, computer, and computer data to be destroyed in a large-scale on a national level</p> <p>(b) is a Cyber Threat that affects or may affect the public order or is a threat to public security or may cause the country or part of the country to be in a critical situation, or an offense regarding terrorism under the Penal Code, battling or war, which an urgent measure is required to maintain the democratic form of government with the King as the Head of the State in accordance with the Constitution of the Kingdom of Thailand, sovereignty and the integrity of the territory, national benefit, compliance with the laws, public safety, normal living of the public, protection of freedom and rights as enshrined in the Constitution and international legislations, public order or benefit, or the protection or remedy of damages from the public disaster that is emergency and critical.</p> <p>An appropriate response, as is necessary and proportionate, is essential in order to deal with a crisis situation.</p>
<p><i>Section 61:</i> When it appears to the CRC that there is or there may be a Cyber Threat at a critical level, the CRC shall issue an order to the Office to perform the following:</p> <ol style="list-style-type: none"> (1) gather information, or relevant documentary evidence, witness, material evidence to analyze the situation, and evaluate the effects from Cyber Threats; (2) support, assist, and participate in the prevention, coping with, and mitigation of risks from Cyber Threats; (3) prevent Cybersecurity Incidents which occurred from Cyber Threats, suggest or issue an order to use the solution system to maintain cybersecurity, including finding the approach for countermeasure or solution regarding cybersecurity; (4) support such that the Office and the relevant organizations, both the public and private sector, to provide assistance and participate in the 	<p><i>Section 61:</i> When it appears to the CRC that there is or there may be a Cyber Threat at a critical level, the CRC shall issue an order to the Office to perform the following:</p> <ol style="list-style-type: none"> (1) gather information, or relevant documentary evidence, witness, material evidence as is necessary and to the extent required to analyze the situation, and evaluate the effects from Cyber Threats; (2) support, assist, and participate in the prevention, coping with addressing, and mitigation of risks from Cyber Threats; (3) prevent Cybersecurity Incidents which occurred from Cyber Threats, suggest or issue an order to use the solution system to maintain cybersecurity, including finding the approach for appropriate countermeasure or solution regarding cybersecurity that respects the privacy of individuals and the integrity of the system at the same time;

<p>prevention, coping with, and mitigation of risks from the Cyber Threats occurred;</p> <p>(5) notify of the Cyber Threat to be informed in general, as necessary and appropriate, taking into consideration the situation, severity, and effect from such Cyber Threat;</p> <p>(6) facilitate in coordinating between relevant Government Agency and private organization to deal with risks and incidents related to cybersecurity.</p>	<p>(4) support such that the Office and the relevant organizations, both the public and private sector, to provide assistance and participate in the prevention, coping with addressing, and mitigation of risks from the Cyber Threats occurred;</p> <p>(5) notify of the Cyber Threat to be informed in general, as necessary and appropriate, taking into consideration the situation, severity, and effect on all stakeholders from such Cyber Threat;</p> <p>(6) facilitate in coordinating between relevant Government Agency and private organization to deal with risks that are accompanied with the imminence of an established threat and incidents related to cybersecurity.</p>
<p><i>Section 62:</i> In operations in accordance with section 61, for the benefit of analyzing the situation and evaluating the effects from Cyber Threats, the Secretary-General shall order the Competent Officials to:</p> <p>(1) issue a letter requesting cooperation from the relevant persons to provide information within an appropriate period and at the prescribed place, or provide information in writing related to the Cyber Threat;</p> <p>(2) issue a letter requesting for information, documents, or copy of the information or documents in the possession of other person which is beneficial to the operation;</p> <p>(3) inquire the persons who has knowledge and understanding of the facts and situations which are related to the Cyber Threat;</p> <p>(4) enter into a property or place of business which is or may be related to the Cyber Threat of a related person or organization, with consent from the person in possession of such place.</p> <p>Any person providing information in accordance with paragraph one, which acts in good faith, shall receive protection and shall not be deemed a wrongful act or a breach of a contract.</p>	<p><i>Section 62:</i> In operations in accordance with section 61, for the benefit of analyzing the situation and evaluating the effects from Cyber Threats strictly in accordance with publicly available criteria that has been set by this Act, the Secretary-General shall order the Competent Officials to:</p> <p>(1) issue a letter requesting cooperation from the relevant persons to provide information within an appropriate period and at the prescribed place, or provide evidence-based information in writing related to the Cyber Threat;</p> <p>(2) issue a letter requesting for information, documents, or copy of the information or documents in the possession of other person which is beneficial to the operation in proving that there is evidence to believe there is a serious risk of harm;</p> <p>(3) inquire the persons who has knowledge and understanding of the facts and situations which are related to the Cyber Threat only as is necessary and proportionate;</p> <p>(4) enter into a property or place of business which is or may be related to the Cyber Threat of a related person or organization, with voluntary consent from the person in possession of such place.</p> <p>A person who gives a true statement according to Paragraph 1 may be protected by the law in the disclosure of such honest information, but only as is necessary and to the extent required.</p>
<p><i>Section 63:</i> In case of necessity to prevent, cope with, and mitigate risks from a Cyber Threat, the CRC shall order the Government Agency to provide information, support its personnel, or use electronic devices under its possession in relation to Maintaining Cybersecurity.</p> <p>The CRC shall ensure that there shall be no use of information under paragraph one that may cause damages and the CRC is responsible for the</p>	<p><i>Section 63:</i> In case of necessity to prevent, cope with address, and mitigate risks from a Cyber Threat, the CRC shall order the Government Agency to provide information, support its personnel, or use electronic devices under its possession in relation to Maintaining Cybersecurity, which it must limit to the extent required to address the threat.</p> <p>The CRC shall ensure that there shall be no use of information under paragraph one that may cause</p>

<p>compensation for the personal, expenses, damages occurred from the use of such electronic devices.</p> <p>Paragraph one and two shall also be applied to the requests to private organization, upon the consent of such private organization.</p>	<p>damages and the CRC is responsible for the compensation for the personal, expenses, damages occurred from the use of such electronic devices. The appropriateness of the action, its extent, the resulting damages, and the reimbursement may be evaluated by the tripartite agency.</p> <p>Paragraph one and two shall also be applied to the requests to private organization, upon the voluntary consent of such private organization.</p>
<p><i>Section 64:</i> In case there is or may be a Cyber Threat at a critical level, the CRC shall prevent, cope with, and mitigate risks from the Cyber Threat and conduct necessary measures.</p> <p>In the operation under paragraph one, the CRC shall issue a letter to the Government Agency which relates to Maintaining Cybersecurity to act or omit any act to prevent, cope with, or mitigate risks from the Cyber Threat properly and efficiently, in accordance with the guideline prescribed by the CRC, including integrating the operation to control, terminate, or mitigate the effect caused by the Cyber Threat in a timely manner.</p> <p>The Secretary-General shall report the operation in accordance with this Section to the CRC constantly and when such Cyber Threat ends, the Secretary-General shall report the operation result to the CRC without delay.</p>	<p><i>Section 64:</i> In case there is or may be a Cyber Threat at a critical level, the CRC shall prevent, cope with address, and mitigate risks from the Cyber Threat and only conduct necessary measures and to the extent required.</p> <p>In the operation under paragraph one, the CRC shall issue a letter to the Government Agency which relates to Maintaining Cybersecurity to act or omit any act to prevent, cope with address, or mitigate risks from the Cyber Threat properly and efficiently, in accordance with the publicly available and accessible guideline prescribed by the CRC, including integrating the operation to control, terminate, or mitigate the effect caused by the Cyber Threat in a timely manner. Remedy shall also apply against the Committees and Offices established under this Act for the misuse, wrongful application or excessive action taken by them in such circumstances including in the form of temporary orders and injunctions; which can be determined by an effective grievance redressal mechanism.</p> <p>The Secretary-General shall report the operation in accordance with this Section to the CRC constantly and when such Cyber Threat ends, the Secretary-General shall report the operation result to the CRC without delay and make the same available to the general public. This shall also include the method of determination of the existence of all possible cybersecurity threat at the critical or crisis level.</p>
<p><i>Section 65:</i> In order to prepare for or remedy damages caused by cybersecurity threats, the Committee has the authority to order the owner of a computer system, computers or the person in charge of the computer system; considered to be affected by or linked to the cybersecurity threat to take the following actions:</p> <ol style="list-style-type: none"> (1) monitor the computer or computer system during a certain period of time; (2) examine the computer or computer system to find an error that affects Maintaining Cybersecurity, analyze the situation, and evaluate the effects from the Cyber Threat; (3) conduct a measure rectifying the Cyber Threat to handle vulnerabilities or remove unwanted 	<p><i>Section 65:</i> In order to prepare for or remedy damages caused by cybersecurity threats, the Committee has the authority to order the owner of a computer system, computers or the person in charge of the computer system; considered to be affected by or linked to the cybersecurity threat to take the following actions unless not in conflict with the protections guaranteed by this Act as well as other related domestic legislation and international standards and obligations:</p> <ol style="list-style-type: none"> (1) monitor the computer or computer systems during a certain period of time, limiting the extent to the period of the existence of or with a reason to believe in the existence of the threat.

<p>programs or terminate and remedy the Cyber Threat that are operating;</p> <p>(4) maintain the status of the computer data or computer system via any methods to operate the computer forensic science;</p> <p>(5) access relevant computer data or computer system or other information related to the computer system only to the extent it is necessary to prevent Cyber Threat.</p> <p>In case of necessity to access information under (5), the CRC shall assign the Secretary- General to submit the motion to the Competent Court to order the owner, the person possessing the computer, the user of the computer or computer system or a person monitoring the computer system in accordance with paragraph one to comply with the motion. The motion submitted to the Court shall specify the cause to believe that a person is performing or will perform an act that cause Cyber Threat in a critical level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay.</p>	<p>(2) examine the computer or computer system to find an error that affects Maintaining Cybersecurity, analyze the situation, and evaluate the effects from the Cyber Threat with due care and in a timely manner;</p> <p>(3) Apply the publicly available and accessible code of practice, in order to mitigate cybersecurity harms, to eliminate malicious software or to suppress the cybersecurity threat. conduct a pre-established and defined measures rectifying the Cyber Threat to handle vulnerabilities or remove unwanted programs or terminate and remedy the Cyber Threat that are operating;</p> <p>(4) Maintain the status of the computer data or computer system via any methods with particular care that it does not harm the integrity of the system and the privacy of individuals, to operate the computer forensic science;</p> <p>(5) Access relevant computer data or computer system or other information related to the computer system only to the extent it is necessary to prevent Cyber Threat.</p> <p>In case of necessity to access information under (5), the CRC shall assign the Secretary- General to submit the motion to the Competent Court or any other independent, impartial and competent judicial authority such as a specialised court established under this Act or through an ombudsperson, to order the owner, the person possessing the computer, the user of the computer or computer system or a person monitoring the computer system in accordance with paragraph one to comply with the motion. The motion submitted to the Court shall specify and prove the cause reason to believe that a person is performing or will perform an act that cause Cyber Threat in a critical level, in addition to the motion being necessary and proportionate to protect a legitimate aim. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay or through an ombudsperson, which shall also be made publicly available. A special Court may also be established under this Act and should include specialized judges who obtain necessary legal and technical expertise, as well as the knowledge of the content and processes of the National Cybersecurity Act in order to consider cases in relation to it.</p>
<p><i>Section 66:</i> In preventing, coping with, or mitigating the risks from Cyber Threats in a critical level, the CRC has the power to order a Competent Official, only to the extent that it is necessary to prevent the Cyber Threat, to do the following:</p> <p>(1) enter into a place to examine, with a letter informing the appropriate reason to the owner or the occupier to examine such place. If there is a cause to believe that there is a computer or</p>	<p><i>Section 66:</i> In preventing, coping with addressing, or mitigating the risks from Cyber Threats in a critical level, the CRC has the power to order a Competent Official, only to the extent that it is necessary and proportionate to prevent the Cyber Threat, to do the following:</p> <p>(1) enter into a place to examine, with a letter informing the appropriate reason to the owner or the occupier to examine such place. If there is a cause to believe due to existing evidence that</p>

computer system related to the Cyber Threat or is affected from the Cyber Threat;

- (2) access the computer data, computer system, or other data related to the computer system, copy, or filter/screen information data or computer program which has a reason to believe that is related to or affected by the Cyber Threat;
- (3) test the operation of the computer or computer system which has a reason to believe that is related to or affected by the Cyber Threat or has been used to search any information from the inside or taking advantage of the computer or computer system;
- (4) seize or freeze a computer, a computer system, or any equipment, only to the extent it is necessary, which has a reason to suspect that is related to the Cyber Threat for the examination or analysis, for not more than thirty days. Once such period is over, computer or any equipment shall be returned to the owner or the person possessing the computer immediately after the examination or analysis is finished.

In operating in accordance with (2), (3), and (4), the CRC may submit a motion to the Competent Court to order the officers to comply with the motion. The motion submitted to the Court shall specify the cause to believe that a person is performing or will perform an act that will cause a Cyber Threat at a critical level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay.

there is a computer or computer system related to the Cyber Threat or is affected from the Cyber Threat;

- (2) access the computer data, computer system, or other data related to the computer system, copy, or filter/screen information data or computer program which has a reason to believe that is related to or affected by the Cyber Threat, **with all personal information and that which would violate privacy removed from the same or with restrictions placed on the handling of such information to appropriately and effectively safeguard it and with notifications provided to third parties that may be affected by such action.**
- (3) test the operation of the computer or computer system which has a reason to believe that is related to or affected by the Cyber Threat or has been used to search any information from the inside or taking advantage of the computer or computer system **only where there is a reason to believe that a risk of harm exists;**
- (4) seize or freeze a computer, a computer system, or any equipment, only to the extent it is necessary **and proportionate**, which has a reason to ~~suspect~~ **believe following clear explanation of the evidence available for such belief** that is related to the Cyber Threat for the examination or analysis, for not more than thirty days. Once such period is over, computer or any equipment shall be returned to the owner or the person possessing the computer immediately after the examination or analysis is finished.

In operating in accordance with (2), (3), and (4), the CRC may submit a motion to the Competent Court to order the officers to comply with the motion. The motion submitted to the Court shall specify the **cause evidence** to believe that a person is performing or will perform an act that will cause a Cyber Threat at a critical level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay. **A special Court may be established under this Act for this purpose and should include specialized judges who obtain necessary legal and technical expertise, as well as the knowledge of the content and processes of the National Cybersecurity Act in order to consider cases in relation to it. This may also be undertaken through an ombudsperson.**



5.3.1. Context

“A digital policy is necessary to protect CII, but such a policy should be applied in a transparent manner, the authorities that apply it should not have a top-down structure, and an insufficient audit system. This is important particularly because of the potential for human rights abuse.”

Klaikong Vaidhyakarn,
Member of Parliament, Future Forward Party



The National Cybersecurity Act of Thailand, while established to prevent, address and mitigate cybersecurity threats should also build a digital environment that Thai netizens and businesses can trust. CII can be supported by the Information and Communication Technology (ICTs) sector and utilized by individuals only when the processes and actions taken provide secure services through CII; in which not just security of information assets and infrastructure is guaranteed but also the rights and interests of users are protected.

This digital environment of trust is however denied at present due to the control mechanisms in the form of government bodies and agencies under the Act. The Act fails to ensure that the functions they carry out under the Act are transparent and they have uncontrolled power, which also stops the realisation of the full potential of economic, social and political opportunities offered by cyberspace.

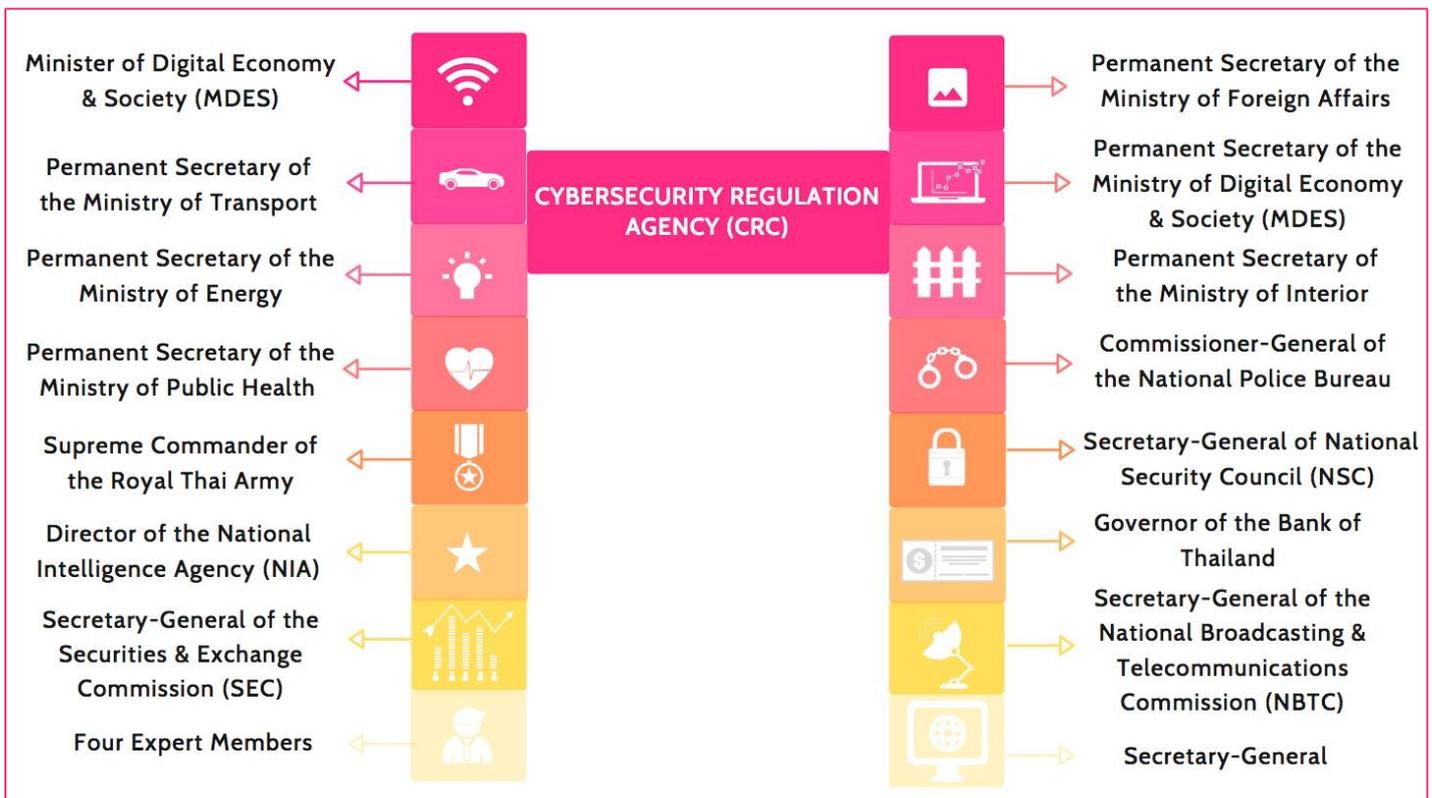
a. Authorities under the Act

Under the Act, various bodies and agencies have been established to carry out its implementation. These include:

1. The National Cybersecurity Committee (NCSC);
2. The Cybersecurity Regulation Committee (CRC);
3. Office of the National Cybersecurity Committee; and
4. The Committee Managing the Office of the National Cybersecurity Committee (CMO).

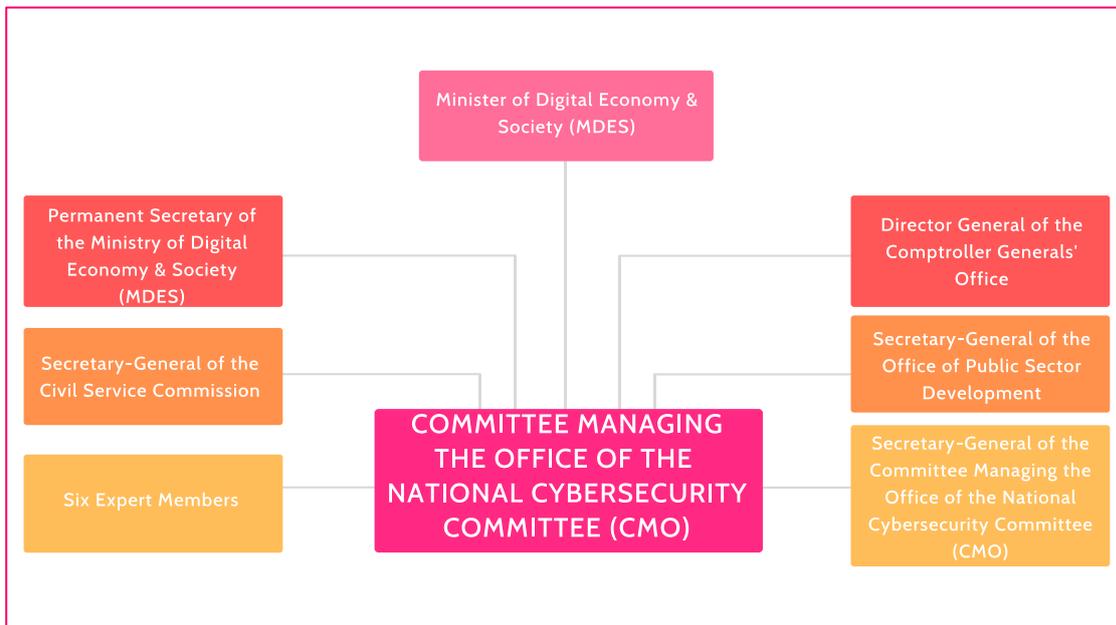
The NCSC, the CRC, the Office of the National Cybersecurity Committee, and the CMO all carry out varied duties in terms of tackling cyberattacks, but in the people that constitute or make up these agencies or bodies there is a lot of overlap, which could be problematic.

The three illustrations below provide an overview of the structure of the NCSC, the CRC, and the CMO as provided in Sections 5, 12, and 25 respectively. These bodies are mostly comprised of government officials whose involvement is considered essential to fulfil their role and responsibilities. To illustrate, the NCSC has a role focused on developing policy such as the national cybersecurity strategy and policy, guidelines and a code of practice under Sections 41, 42, and 43; and the CRC with the support of the CMO primarily executes this policy proposed by the NCSC and takes specific action following a risk assessment that establishes the occurrence of an actual or possible cybersecurity threats as set out in Sections 61, 62, 63, 64, 65, and 66 of the Act.



Therefore, to support their ability to carry out these roles, the **15-member NCSC** is chaired by the Prime Minister and is made up of Ministers and Permanent Secretaries from the Ministries which are believed to have the expertise to draft supporting policy, along with those that have security threat response knowledge, namely the Commissioner- General of the National Police Bureau and the Secretary-General of the National Security Council (NSC). The **19-member CRC** on the other hand is made up of Permanent Secretaries from all Ministries with portfolios or representatives from government organizations or regulatory bodies that cover areas also considered critical infrastructure as identified by Section 49 namely *national security, public services, banking and finance, information technology, and telecommunication, transportation, energy and public utilities, and public health*. The reason for this is to make it easier during the response taken and in order to support CII that are victims of cybersecurity threats.

However, this could also be challenging as while those part of the NCSC and the CRC could be skilled in their role, their focus remains primarily at the highest levels and may not necessarily give them the expertise to understand or represent the perspectives of civil society, the technical community, and private sector entities that could be affected. Thus, all policy developed and actions taken could be taken only to benefit the government in order for them to maintain control, without any alternative opinion allowed to ensure accountability. Further, any misuse or misinterpretation that these individuals are contributing to in their non-cybersecurity work could be replicated here. For instance, some individuals that make up the CRC including the Permanent Secretary of the MDES, and the Permanent Secretary of the Ministry of Public Health are also going to be part of a newly comprised Anti-Fake news Centre.⁴⁸ Although the purpose of this Centre is to tackle fake facts on the internet, but based on practices in other ASEAN countries and the trend in the behaviour of the government, there is a fear that this information could be used to discredit information provided by critics or oppositions groups. Being a part of the CRC will give the Permanent Secretary of the MDES and the Permanent Secretary of the Ministry of Public Health, the opportunity to misuse the power under the National Cybersecurity Act to propagate their agenda of silencing dissent in the digital sphere.



While the NCSC, CRC, and the CMO require the inclusion of experts as honorary directors based on expertise and experience in maintaining cybersecurity, information technology and communications, protection of data privacy, science, engineering, law, finance or other related fields, there is no mention that these experts need to be independent and must represent all stakeholder groups in a balanced manner, so that the Act is beneficial to all those affected. This can only be achieved if their selection is done in a transparent manner and based on clear, publicly available criteria that can be reviewed by the neutral tripartite agency envisioned by the recommended amendments.

b. Responsibilities of the authorities

Section 9 of the Act sets out the primary duties and responsibilities of the NCSC, including by (1) proposing cybersecurity policy and strategy; (2) prescribing management policies on maintaining cybersecurity to the government agency and organizations of CII; (3) preparing the operational plan for maintaining cybersecurity where cybersecurity threats may occur or have occurred; (4) prescribing minimum standards and guidelines to improve cybersecurity service systems; (5) prescribing measures and guidelines to enhance maintaining cybersecurity skills to officials and staff from Organizations of CIIs, government agencies, supervising or regulating organizations, and private organizations; (5) developing a framework for cooperation with domestic and international organizations to tackle cybersecurity threats collectively; (6) monitoring supervising or regulating organizations, government agency, or the organization of CIIs, to develop cybersecurity policies and frameworks for them; (7) monitoring and evaluating the implementation of cybersecurity policies and frameworks on maintaining cybersecurity under the Act; (8) making recommendations to the Digital Economy and Society Committee or to the Council of Ministers on maintaining cybersecurity; and (9) publishing reports on the outcomes of practices, law and policy related to maintaining cybersecurity.

Section 13 and 22 of the Act set out the primary duties and responsibilities of the CRC, for which they may be supported by the CMO, including by (1) functioning as the National Centre for Cooperation and Maintenance of Cybersecurity; (2) monitoring and executing policies and strategies proposed by the CMO; (3) conducting surveillance and responding to cybersecurity incidents; (4) making an announcement about cybersecurity threats; (5) cooperating with organizations managing information systems to work on cybersecurity concerns; (6) imposing guidelines and standards to maintain cybersecurity from the stage of risk assessment to response, for public organizations and organizations managing information systems; (7) organizing the development of prevention and response protocols by organizations managing information systems and ISPs; (8) cooperating with the State and private organizations in order to respond to cybersecurity threats; (9) acting as the National Research Centre for Cybersecurity Analysis by researching and analyzing essential information about cybersecurity concerns and by disseminating of information about cybersecurity issues or incidents; (10) educating on cybersecurity legislations and the maintenance of cybersecurity; (11) categorising threat levels to determine ways to prevent, protect, monitor, and resolve cybersecurity harms based on its severity; and (12) cooperating, supporting and assisting organizations that are responsible for cybersecurity policies, preventive measures, and strategies such as the NCSC.

All policies proposed and actions taken by the NCSC, CRC and CMO should not continue to have extensive gaps like they do now. This can be achieved if policies and action are evidence-based and with clear reasons, precise, comprehensive, publicly available and accessible, include guarantees of procedural fairness such as user notification on risks and access to personal information, follow due process, undertaken only to the extent that is necessary and proportional to the legitimate aim to be achieved, utilize innovative and collaborative steps where possible, respect the integrity of information and information systems, ensure responses are directed at cybersecurity incidents that have been identified based on clear evaluation and publicly available criteria, include and consult all stakeholders such as authorities and officials identified under this Act as well as private sector entities and technical experts, not compel the violation of rights, include technical perspectives, and with periodic review for lawfulness carried out by an independent multi-stakeholder mechanism.

“Sound policies, strategies and legislation must be complimented by the government establishing organizational structures that clearly define roles and with multi-stakeholder cooperation being nurtured at a national, regional, and international level.”

Sameer Sharma,
Senior Advisor, International
Telecommunications Union (ITU)
Regional Office for Asia Pacific

Further, in carrying out all the responsibilities stated above, the only oversight over the power of the NCSC that exists is the Cabinet, since the proposals are submitted to them for approval. However, since the NCSC is chaired by the Prime Minister – his or her Cabinet would not oppose any policy proposal put forward by a body he is a part of. With respect to the CRC and CMO, the NCSC has oversight but all this points to the situation where all views will be focused towards achieving the goals of the NCSC, even if the goal is to ensure political security or retention of the power by the Prime Minister and his government. **This will have to be addressed through the proposed creation of an independent multi-stakeholder monitoring mechanism that carries out audits through regular monitoring and evaluation, in order to determine the efficiency in implementation of the Act. The report produced and the input provided could also be used as a basis to review the content and gaps in the National Cybersecurity Act periodically to account for any shortcomings, as well as for the development in technology, changing cyber capabilities, and the developing need of society.**

c. The case of the Office of the National Cybersecurity Agency and its juristic status

The NCSA poses a unique challenge in the power it exercises also because of its status as recognized in Section 20 and the exemptions it enjoys with respect to its actions as a result, according to Section 21. To explain, Section 20 of the Act states that the Office of the National Cybersecurity Agency shall be set up as a public organization with its status as a juristic person, and not as a State agency under the Government Administration Act or as a State enterprise in terms of funding. This would not allow to hold the Office of the National Cybersecurity Agency responsible for violations under administrative laws that protect against misuse of power. This could only be addressed if for the purposes of accountability, the content of the National Government Organization Act of 1991 is integrated into the guidelines of operation or the code of practice that govern the actions of the NCSA.

Additionally, the other challenge in the Act is that it also provides for exemption of the activities of the Office of the National Cybersecurity Agency from the laws on labour protection, the law on labour relations, the law on social security, and the law on compensation with the employees only receiving the compensation set out in these legislations, with no ability to question it. Such unchecked power not just outside but within the Office of the National Cybersecurity Agency and its misuse in its employment practices must also be resolved.

5.3.2. Recommended Amendments

Original Text (in sequential order)	Suggested Changes , Deletions and Additions to the National Cybersecurity Act
<p><i>Section 5:</i> There shall be a committee named the “National Cybersecurity Committee” abbreviated as “NCSC.” The NCSC shall be comprised of:</p> <ol style="list-style-type: none"> (1) The Prime Minister as a chairperson; (2) directors by position, comprising the Minister of Defense, Minister of Digital Economy and Society, Permanent Secretary of the Ministry of Finance, Permanent Secretary of the Ministry of Justice, Commissioner-General of the National Police Bureau, and Secretary-General of the National Security Council; (3) honorary directors not exceeding seven persons appointed by the Cabinet based, who have knowledge, expertise, and remarkable experience in Maintaining Cybersecurity, information technology and communications, protection of data privacy, science, engineering, law, finance or other relevant aspects that are beneficial to Maintaining Cybersecurity. <p>The criteria and selection methods for the persons to be proposed to the Cabinet as honorary directors, including the selection of honorary directors to stay in the office in replacement of a person who vacated the office prior to the expiry of the term in accordance with section 7 paragraph two shall be in accordance with the rules as determined by the Cabinet as suggested by the Committee.</p>	<p><i>Section 5:</i> There shall be a committee named the “National Cybersecurity Committee” abbreviated as “NCSC.” The NCSC shall be comprised of:</p> <ol style="list-style-type: none"> (1) The Prime Minister as a chairperson; (2) directors by position, comprising the Minister of Defense, Minister of Digital Economy and Society, Permanent Secretary of the Ministry of Finance, Permanent Secretary of the Ministry of Justice, Commissioner-General of the National Police Bureau, and Secretary-General of the National Security Council; (3) honorary directors not exceeding seven independent persons with balanced representation from various stakeholder groups appointed by the Cabinet based, who have knowledge, expertise, and remarkable experience in Maintaining Cybersecurity, information technology and communications, protection of data privacy, science, engineering, law, finance or other relevant aspects that are beneficial to Maintaining Cybersecurity. <p>The criteria and selection methods for the persons to be proposed to the Cabinet as honorary directors, including the selection of honorary directors to stay in the office in replacement of a person who vacated the office prior to the expiry of the term in accordance with section 7 paragraph two shall be in accordance with the rules made publicly available as well as accessible as determined by the Cabinet as suggested by the Committee.</p>
<p><i>Section 6:</i> Honorary directors in the Committee must have Thai nationality and shall not possess the following prohibited characteristics</p>	<p><i>Section 6:</i> Honorary directors in the Committee must have Thai nationality and shall not possess the following prohibited characteristics based on an independent and transparent assessment</p>
<p><i>Section 9:</i> The Committee shall have the following duties and powers to:</p> <ol style="list-style-type: none"> (1) propose the policy and plan on Maintaining Cybersecurity, promote, and support the act of Maintaining Cybersecurity in accordance with section 42 and section 43 for the Cabinet’s approval, which shall be in accordance with the guideline specified under section 42; (2) determine management policy for Maintaining Cybersecurity for the Government Agency and Organization of Critical Information Infrastructure; (3) prepare the operational plan for Maintaining Cybersecurity to propose to the Cabinet as a master plan for Maintaining Cybersecurity under 	<p><i>Section 9:</i> The Committee shall have the following duties and powers to:</p> <ol style="list-style-type: none"> (1) propose the evidence-based cybersecurity policies and strategies, in line with Section 42, Section 43, on receiving the approval of the Council of Ministers according to Section 42; (2) determine management policy for Maintaining Cybersecurity for the Government Agency and Organization of Critical Information Infrastructure only to the extent that is necessary and proportionate with approaches that are collaborative and respect the integrity of communications and systems; (3) prepare the operational plan for Maintaining Cybersecurity to propose to the Cabinet as a

general situations and situations where the Cyber Threats may occur or have occurred; such plan shall be in accordance with the policy, strategy, and national plan as well as the policy framework and master plan which are related to maintaining the security of the National Security Council;

- (4) establish the standard and guideline to enhance and develop service systems pertaining to Maintaining Cybersecurity, establish the standard in respect of Maintaining Cybersecurity, and determine the minimum standard pertaining to a computer, computer system, computer program, as well as support the certifying of standards for Maintaining Cybersecurity of Organization of Critical Information Infrastructure, Government Agency, Supervising or Regulating Organization, and private organizations;
- (5) prescribe measures and guidelines to enhance the knowledge and expertise in Maintaining Cybersecurity of the Competent Officials, officers of the Organization of Critical Information Infrastructure, Government Agency, Supervising or Regulating Organization, and private organizations which are related to Maintaining Cybersecurity;
- (6) set out a framework on coordinating with other agencies, both in the country and foreign countries, which are related to Maintaining Cybersecurity;
- (7) appoint and remove the Secretary-General;
- (8) assign the supervision and regulation, including the issuing of regulations, objectives, duties and power, and the operational framework regarding Maintaining Cybersecurity to the Supervising or Regulating Organization, Government Agency, or the Organization of Critical Information Infrastructure;
- (9) monitor and evaluate the results of operating in accordance with the policy and plan on Maintaining Cybersecurity, operational plan for Maintaining Cybersecurity, and of Maintaining Cybersecurity as specified under this Act;
- (10) suggest and provide opinions to the Digital Economy and Society Committee or to the Cabinet on Maintaining Cybersecurity;
- (11) suggest to the Cabinet the legislation or amendment of laws related to Maintaining Cybersecurity;
- (12) prepare a summary report of undertakings of Maintaining Cybersecurity that have significant effect, or the approach for developing the standard of Maintaining Cybersecurity for the Cabinet to be informed;
- (13) perform any other task as specified under this Act or as assigned by the Cabinet.

master plan for Maintaining Cybersecurity under general situations and situations where the Cyber Threats may occur or have occurred **as clearly evaluated and identified through publicly available criteria**; such plan shall be in accordance with the policy, strategy, and national plan as well as the policy framework and master plan which are related to maintaining the security of the National Security Council **while respecting other domestic and international law and policy standards**;

- (4) establish the standard and guideline to enhance and develop service systems pertaining to Maintaining Cybersecurity, establish the **precise** standard in respect of Maintaining Cybersecurity, and determine the minimum standard pertaining to a computer, computer system, computer program, as well as support the certifying of standards for Maintaining Cybersecurity of Organization of Critical Information Infrastructure, Government Agency, Supervising or Regulating Organization, and private organizations;
- (5) prescribe **publicly available and accessible** measures and guidelines to enhance the knowledge and expertise in Maintaining Cybersecurity of the Competent Officials, officers of the Organization of Critical Information Infrastructure, Government Agency, Supervising or Regulating Organization, and private organizations, **as well as amongst authorities and officials** which are related to Maintaining Cybersecurity;
- (6) set out a **comprehensive** framework on coordinating with other agencies, **private sector entities and technical experts** both in the country and foreign countries, which are related to Maintaining Cybersecurity **which is however subject to the guarantees of procedural fairness**;
- (7) appoint or remove the Secretary-General **with a legitimate cause**;
- (8) assign the supervision and regulation, including the issuing of regulations, objectives, duties and power, and the operational framework **as is necessary and proportional** regarding Maintaining Cybersecurity to the Supervising or Regulating Organization, Government Agency, or the Organization of Critical Information Infrastructure **following consultation with them**;
- (9) monitor and evaluate the results of operating in accordance with the policy and plan on Maintaining Cybersecurity, operational plan for Maintaining Cybersecurity, and of Maintaining Cybersecurity as specified under this Act, **with results used for the periodic review of these policies and frameworks**;
- (10) suggest and provide opinions to the Digital Economy and Society Committee or to the Cabinet on Maintaining Cybersecurity;

	<ul style="list-style-type: none"> (11) suggest to the Cabinet the legislation or amendment of laws related to Maintaining Cybersecurity; (12) prepare a summary report of undertakings of Maintaining Cybersecurity that have significant effect, or the approach for developing the standard of Maintaining Cybersecurity for the Cabinet to be informed, while making them publicly available; (13) perform any other task as specified under this Act or as assigned by the Cabinet, subject to periodic assessment on its lawfulness by the tripartite agency.
<p><i>Section 10:</i> The meeting of the Committee shall be in accordance with the rules as determined by the Committee, where the meeting may proceed via electronic means or other means.</p>	<p><i>Section 10:</i> The meeting of the Committee shall be in accordance with the rules as determined by the Committee, where the meeting may proceed via electronic means or other means, as well as with international standards and legislations through transparent processes.</p>
<p><i>Section 12:</i> In undertaking the duty and power of the Committee in accordance with section 9, there shall be a Cybersecurity Regulating Committee abbreviated as "CRC," comprising:</p> <ul style="list-style-type: none"> (1) the Minister of the Digital Economy and Society as a chairperson; (2) directors by position, comprising the Permanent Secretary of the Ministry of Foreign Affairs, Permanent Secretary of the Ministry of Transport, Permanent Secretary of the Ministry of Digital Economy and Society, Permanent Secretary of the Ministry of Energy, Permanent Secretary of the Ministry of Interior, Permanent Secretary of the Ministry of Public Health, Commissioner-General of the National Police Bureau, Supreme Commander, Secretary-General of the National Security Council, Director of the National Intelligence Agency, Governor of the Bank of Thailand, Secretary-General of the Securities and Exchange Commission, and the Secretary-General of the National Broadcasting and Telecommunications Commission; (3) honorary directors not exceeding four persons, who are appointed by the Committee among the persons who have knowledge, expertise, and experience which is remarkable and beneficial to Maintaining Cybersecurity. <p>The criteria and selection methods for the appropriate persons to appoint as honorary directors shall comply with the rules as determined by the Committee.</p>	<p><i>Section 12:</i> In undertaking the duty and power of the Committee in accordance with section 9, there shall be a Cybersecurity Regulating Committee abbreviated as "CRC," comprising:</p> <ul style="list-style-type: none"> (1) the Minister of the Digital Economy and Society as a chairperson. (2) directors by position, comprising the Permanent Secretary of the Ministry of Foreign Affairs, Permanent Secretary of the Ministry of Transport, Permanent Secretary of the Ministry of Digital Economy and Society, Permanent Secretary of the Ministry of Energy, Permanent Secretary of the Ministry of Interior, Permanent Secretary of the Ministry of Public Health, Commissioner-General of the National Police Bureau, Supreme Commander, Secretary-General of the National Security Council, Director of the National Intelligence Agency, Governor of the Bank of Thailand, Secretary-General of the Securities and Exchange Commission, and the Secretary-General of the National Broadcasting and Telecommunications Commission; (3) honorary directors not exceeding four independent persons representing different stakeholder groups including the private sector and civil society, who are appointed by the Committee among the persons who have knowledge, expertise, and experience which is remarkable and beneficial to Maintaining Cybersecurity. <p>The criteria and selection methods for the appropriate persons to appoint as honorary directors shall comply with the rules as determined by the Committee that are made publicly available.</p>

	<p>The clear criteria and selection methods for the appropriate persons to appoint as honorary directors shall comply with the rules as determined by the Committee.</p>
<p><i>Section 13:</i> The CRC shall have the following duties and powers:</p> <ol style="list-style-type: none"> (1) monitor the undertaking in accordance with the policy and plan according to section 9 (1) and section 42; (2) monitor and undertake in order to cope with Cyber Threats at critical level in accordance with section 61, section 62, section 63, section 64, section 65, and section 66; (3) regulate the undertaking of the national coordinating agencies for the security of computer systems and the incident response and computer forensic science; (4) determine the Code of Practice and standard framework in Maintaining Cybersecurity which are the minimum requirement in the act of Maintaining Cybersecurity for the Government Agency and the Organization of Critical Information Infrastructure, including determining the measure for risk assessment of, responses to, and coping with the Cyber Threats when there are any Cyber Threats or incidents that affect or may significantly or severely affect or damage the information system of the country for the quick, efficient, and united act of Maintaining Cybersecurity; (5) determine the duties of Organization of Critical Information Infrastructure and duties of the Supervising or Regulating Organization which should at least determine the duties for the Supervising or Regulating Organization to determine the appropriate standards for each Organization of Critical Information Infrastructure and Government Agency in coping with Cyber Threats; (6) prescribe the level of Cyber Threats including the details of the measures to prevent, cope with, assess, suppress, and suspend the Cyber Threats at each level to present to the Committee; (7) analyze the situation and evaluate the effect from Cyber Threats, in order to propose to the Committee to consider issuing an order, in the case there is or may be an occurrence of a Cyber Threat in a level that is more critical. <p>In determining the standard framework according to paragraph one (4), the risk management principals shall be considered, which shall contain at least the approaches and measures as follows:</p> <ol style="list-style-type: none"> (1) specification of the risk that may occur to the computer, computer data, computer system, other information related to computer system, property, and life and body of a person; 	<p><i>Section 13:</i> The CRC shall have the following duties and powers:</p> <ol style="list-style-type: none"> (1) monitor the undertaking in accordance with the evidence-based policy and plan according to section 9 (1) and section 42; (2) monitor and undertake in order to cope with address Cyber Threats through comprehensive evaluation and identification using publicly available criteria to determine if a threat is at critical level in accordance with section 61, section 62, section 63, section 64, section 65, and section 66 only to the extent that is necessary and proportional, following due process, notifying users, and respecting the integrity of communications and systems; (3) regulate the undertaking of the national coordinating agencies for the security of computer systems and the incident response and computer forensic science; (4) determine the comprehensive and publicly available Code of Practice and standard framework in Maintaining Cybersecurity which are the minimum requirement in the act of Maintaining Cybersecurity for the Government Agency and the Organization of Critical Information Infrastructure, including determining the measure for risk assessment of, responses to, and coping with addressing the Cyber Threats when there are any Cyber Threats or incidents that affect or may significantly or severely affect or damage the information system of the country for the quick, efficient, and united act of Maintaining Cybersecurity while retaining the integrity of these systems and integrating the input of relevant stakeholders; (5) determine the duties of Organization of Critical Information Infrastructure and duties of the Supervising or Regulating Organization which should at least proactively determine the duties for the Supervising or Regulating Organization to determine the appropriate standards for each Organization of Critical Information Infrastructure and Government Agency in coping with addressing Cyber Threats as is necessary and to the extent required, without compelling the violation of individual rights; (6) prescribe the level of Cyber Threats using clear evaluation and identification through publicly available criteria; including the details of the measures to prevent, cope with address, assess, suppress, and suspend the Cyber Threats at each level to present to the Committee subject to

<p>(2) measures to prevent the risk that may occur;</p> <p>(3) measures to examine and monitor the Cyber Threats;</p> <p>(4) measures to respond when the Cyber Threats are detected;</p> <p>(5) measures to remedy and restore the damage occurred from a Cyber Threat.</p>	<p>periodic assessment on its lawfulness by the tripartite agency;</p> <p>(7) analyze the situation and evaluate the effect from Cyber Threats, in order to propose to the Committee to consider issuing an order, in the case there is or may be an occurrence of a Cyber Threat in a level that is more critical with results used for the review of cybersecurity policies and frameworks.</p> <p>In determining the standard framework according to paragraph one (4), the risk management principals balanced with the respect for individual rights and technical capabilities shall be considered, which shall contain at least the approaches and measures as follows:</p> <p>(1) specification of the legitimate risk that may occur to the computer, computer data, computer system, other information related to computer system, property, and life and body of a person;</p> <p>(2) measures to prevent the risk that may occur that are legitimate and applied to situations where there is a reason to believe that a threat may exist;</p> <p>(3) measures to clearly examine and credibly monitor the Cyber Threats in situations where there is evidence to believe that there may be a risk of serious harm;</p> <p>(4) measures to respond when the Cyber Threats are detected as necessary and proportionate;</p> <p>(5) measures to remedy and restore the damage occurred from a Cyber Threat.</p>
<p><i>Section 14:</i> In order to act in accordance with section 13 paragraph one (2) to cope with Cyber Threats in a timely manner, the CRC may assign the Minister of the Digital Economy and Society, Supreme Commander, and other directors as determined by the CRC to jointly perform such duty, and may determine that the Supervising or Regulating Organization and the threatened Organization of Critical Information Infrastructure shall join in order to act, coordinate, and provide support.</p> <p>The performance under paragraph one shall be in accordance with the rules prescribed by the CRC.</p>	<p><i>Section 14:</i> In order to act in accordance with section 13 paragraph one (2) to cope with address Cyber Threats in a timely manner, the CRC may assign the Minister of the Digital Economy and Society, Supreme Commander, and other directors as determined by the CRC to jointly perform such duty, and may determine that the Supervising or Regulating Organization and the threatened Organization of Critical Information Infrastructure shall join in order to act, coordinate, and provide support.</p> <p>The performance under paragraph one shall be in accordance with the rules prescribed by the CRC subject to review by the tripartite agency that will guarantee procedural fairness.</p>
<p><i>Section 15:</i> The provision of section 6, section 7, and section 8 shall be applied to the honorary directors in the CRC mutatis mutandis.</p>	<p><i>Section 15:</i> The provision of section 6, section 7, and section 8 shall be applied to the honorary directors in the CRC mutatis mutandis using transparent methods.</p>
<p><i>Section 16:</i> The CRC shall have the power to appoint the sub-committee to perform any tasks as assigned by the CRC.</p>	<p><i>Section 16:</i> The CRC shall have the power to appoint the sub-committee that is qualified and publicly identified to perform any tasks as assigned by the CRC.</p>

<p><i>Section 17:</i> The meeting of the CRC and the sub-committee shall be in accordance with the rules as determined by the CRC, where the meeting may proceed via electronic means or other means.</p>	<p><i>Section 17:</i> The meeting of the CRC and the sub-committee shall be in accordance with the publicly available and accessible rules as determined by the CRC, where the meeting may proceed via electronic means or other means and documented.</p>
<p><i>Section 19:</i> In order to perform the duties in accordance with this Act, the Competent Official shall present his/her identification card to the relevant person.</p> <p>In the appointment of the Competent Official, the Minister shall consider appointing a person with the knowledge and expertise in Maintaining Cybersecurity to be the Competent Official to perform any tasks under this Act. The level of such knowledge and expertise of the Competent Official shall be in accordance with the notification prescribed by the CRC.</p> <p>The identification card issued to the Competent Official shall be in accordance with the notification prescribed by the CRC.</p>	<p><i>Section 19:</i> In order to perform the duties in accordance with this Act, the Competent Official shall present his/her identification card to the relevant person.</p> <p>In the appointment of the Competent Official, the Minister shall consider appointing a person with the proven knowledge and expertise in Maintaining Cybersecurity to be the Competent and independent Official to perform any tasks under this Act. The level of such knowledge and expertise of the Competent Official shall be in accordance with the notification prescribed by the CRC.</p> <p>The identification card issued to the Competent Official shall be in accordance with the publicly available and accessible notification prescribed by the CRC.</p>
<p><i>Section 20:</i> There shall be an Office of the National Cybersecurity Committee as a Government Agency who is a juristic person and not a government sector entity under the laws governing the administration or a state enterprise under the law on budget procedures or other laws.</p>	<p><i>Section 20:</i> There shall be an Office of the National Cybersecurity Committee as a Government Agency who is a juristic person and not a government sector entity under the laws governing the administration or a state enterprise under the law on budget procedures or other laws. However, for the purposes of accountability, the practices and procedures of the Office of the National Cybersecurity Agency shall be subject to regulation of the National Government Organization Act, 1991 the content of which shall be integrated into the guidelines for their operation.</p>
<p><i>Section 21:</i> The operation of the Office is not regulated by the labor protection law, labor relation law, social security law, and compensation fund law. However, officers and employees of the Office shall receive compensation not less than that specified under the labor protection law, social security law, and compensation fund law.</p>	<p><i>Section 21:</i> The operation of the Office is not regulated by the labor protection law, labor relation law, social security law, and compensation fund law. However, officers and employees of the Office shall strictly receive compensation not less than that specified under the labor protection law, social security law, and compensation fund law.</p>
<p><i>Section 22:</i> The Office shall be responsible for administrative, academic, meeting, and secretarial tasks of the Committee and the CRC, and shall also have the duties and powers to:</p> <ol style="list-style-type: none"> (1) suggest and support preparation of the policy and plan on Maintaining Cybersecurity and the operational plan for Maintaining Cybersecurity in accordance with section 9 to the Committee; (2) prepare the Code of Practice and standard framework in Maintaining Cybersecurity in accordance with section 13 paragraph one (4), proposed to the CRC for the approval; (3) coordinate the acts of Maintaining Cybersecurity of Organization of Critical Information 	<p><i>Section 22:</i> The administration, research, and organizational teams of the Office; the Secretary of the NCSC, and the Cybersecurity Regulation Committee have the duty and responsibility to undertake the following:</p> <ol style="list-style-type: none"> (1) suggest and support preparation of the evidence-based policy and plan on Maintaining Cybersecurity and the operational plan for Maintaining Cybersecurity in accordance with section 9 to the Committee; (2) prepare the Code of Practice and standard comprehensive and publicly available framework in Maintaining Cybersecurity in accordance with section 13 paragraph one (4), proposed to the CRC for the approval;

Infrastructure in accordance with section 53 and section 54;

- (4) coordinate and cooperate in the establishment of coordinating agencies for Maintaining Cybersecurity in the country and foreign countries with respect to Cybersecurity Incidents and determining Cybersecurity Solutions;
- (5) act and coordinate with the Government Agency and private organizations in order to respond and cope with the Cyber Threats as assigned by the Committee;
- (6) monitor the risk of occurrence of Cyber Threats, follow, analyze, and process information in relation to the Cyber Threats and the alerts on the Cyber Threats;
- (7) perform, coordinate, support, and assist relevant agencies in complying with the policy and plan on Maintaining Cybersecurity, the operational plan for Maintaining Cybersecurity, and the measures to prevent, cope with, and mitigate the risks at Cyber Threats or as ordered by the Committee;
- (8) act and cooperate or assist in preventing, coping with, and mitigating the risks of Cyber Threats, especially Cyber Threats that affect or occur in relation to the Critical Information Infrastructure;
- (9) strengthen the knowledge and understanding in Maintaining Cybersecurity, including to create awareness of the incidents regarding the Cyber Threats in order to have a practical operation in a manner that is integrated and up-to-date;
- (10) act as central point of collection and analysis of data regarding Maintaining Cybersecurity of the country, and disseminating the information related to cybersecurity risks and incidents to Government Agencies and private organizations;
- (11) act as the central coordinator between the institution regarding Maintaining Cybersecurity of Government Agencies and private organizations, both in the country and in foreign countries;
- (12) make agreements and cooperate with organizations or institutions both in the country and in foreign countries for the operation in accordance with the duty and power of the Office, upon receiving approval from the Committee;
- (13) study and research necessary information required for Maintaining Cybersecurity, in order to prepare recommendations on measures for Maintaining Cybersecurity, including providing relevant agencies with training and practice for coping with the Cyber Threats;
- (14) enhance, support, and act in order to disseminate knowledge regarding Maintaining Cybersecurity, and provide trainings to enhance the skills and expertise in performing duties in relation to Maintaining Cybersecurity;
- (15) report the progress and situation for the execution of this Act including the problems, obstacles, and proposal to the Committee to

- (3) coordinate the acts of Maintaining Cybersecurity of Organization of Critical Information Infrastructure in accordance with Section 53 and Section 54 **as is necessary and to the extent required, without compelling the violation of individual rights**;
- (4) coordinate and cooperate in the establishment of coordinating agencies for Maintaining Cybersecurity in the country and foreign countries with respect to Cybersecurity Incidents and determining Cybersecurity Solutions **domestically and also addresses international cybersecurity issues that have a negative domestic impact**;
- (5) act and coordinate with the Government Agency and private organizations in order to respond and ~~cope with~~ **address** the Cyber Threats as assigned by the Committee, **and that meets the criteria of necessity and proportionality**;
- (6) monitor the risk of occurrence of Cyber Threats, follow, analyze, and process information in relation to the Cyber Threats and the alerts on the Cyber Threats **through clear identification under publicly available criteria in situations where there is a evidence to believe that there may be a risk of serious harm, along with the reason behind such an identification**;
- (7) perform, coordinate, support, and assist relevant agencies in complying with the policy and plan on Maintaining Cybersecurity, the operational plan for Maintaining Cybersecurity, and the **legitimate** measures to prevent, ~~cope with~~ **address**, and mitigate the risks at Cyber Threats or as ordered by the Committee, **in line with other relevant and related domestic as well as international standards and legislations, in situations where there is a reason to believe that a threat may exist without determining this imminence of a threat by analysing the content of information**;
- (8) act and cooperate or assist **only as far as necessary**, in preventing, coping with, and mitigating the risks of Cyber Threats **in situations where there is evidence to believe that there may be a risk of serious harm**, especially Cyber Threats that affect or occur in relation to the Critical Information Infrastructure;
- (9) strengthen the knowledge **of all government agencies and authorities under the National Cybersecurity Act** and understanding in Maintaining Cybersecurity, including to create awareness of the incidents regarding **cybercrimes, digital issues**, the Cyber Threats in order to have a practical operation in a **innovative and collaborative** manner that is integrated and up-to-date;
- (10) act as central point of collection and analysis of data regarding Maintaining Cybersecurity of the country, and disseminating the **accurate legal and technical** information related to

consider to proceed according to the period as determined by the Committee;

- (16) perform any other task related to Maintaining Cybersecurity of the country as assigned by the Committee or the Cabinet.

For the benefit of acting according to the duties and powers in accordance with (6), the Office shall establish a national coordinating agency for maintaining the security of computer systems as an internal department of the Office, which shall have duties and powers as determined by the Committee.

cybersecurity risks and incidents to [implementing officials as well as](#) Government Agencies and private organizations;

- (11) act as the central coordinator between the institution regarding Maintaining Cybersecurity of Government Agencies and private organizations, [civil society, technical experts](#) both in the country and in foreign countries;
- (12) make agreements and cooperate with organizations or institutions both in the country and in foreign countries for the operation in accordance with the duty and power of the Office, upon receiving approval from the Committee [so as to benefit information systems, assets and individuals](#);
- (13) study and research necessary information required for Maintaining Cybersecurity, in order to prepare recommendations on [legitimate](#) measures for Maintaining Cybersecurity, including providing relevant agencies with training and practice for coping with the Cyber Threats, [in situations where there is a reason to believe that a threat may exist that must be determined without assessing the content of information, but with a tripartite agency in place to monitor such preventive measures and an ombudsperson considering complaints in this respect](#);
- (14) enhance, support, and act in order to disseminate knowledge regarding Maintaining Cybersecurity [amongst all government agencies and authorities under the National Cybersecurity Act](#), and provide trainings to enhance the skills and expertise in performing duties in relation to Maintaining Cybersecurity, [technical aspects and individual rights](#);
- (15) report the progress and situation for the execution of this Act including the problems, obstacles, and proposal to the Committee to consider to proceed according to the period as determined by the Committee, [complying with standards off procedural fairness through steps such as user notification and integrity of systems involved](#);
- (16) perform any other task related to Maintaining Cybersecurity of the country as assigned by the Committee or the Cabinet, [subject to periodic assessment on its lawfulness by the tripartite agency](#).

For the benefit of acting according to the duties and powers in accordance with (6), the Office shall establish a national coordinating agency for maintaining the security of computer systems as an internal department of the Office, which shall have duties and powers as determined by the Committee, [subject to periodic assessment on its lawfulness by the tripartite agency](#).

<p><i>Section 24:</i> Money and properties of the Office under paragraph one must be provided to the treasury as national revenue.</p>	<p><i>Section 24:</i> Money and assets of the Office according to (1) are to be publicly disclosed and delivered to the treasury as income of the State.</p>
<p><i>Section 25:</i> There shall be a Committee Managing the Office of the National Cybersecurity Committee, abbreviated as "CMO," to supervise the general administration of the Office, consisting of the Minister of the Digital Economy and Society as the chairperson, Permanent Secretary of the Ministry of Digital Economy and Society, Director General of the Controller General's Department, the Secretary-General of the Civil Service Commission, the Secretary-General of the Office of the Public Sector Development, and honorary directors not exceeding six persons to be directors.</p> <p>The honorary directors under paragraph one shall be appointed by the Cabinet among the persons who have knowledge, expertise, and remarkable competency in Maintaining Cybersecurity, information technology and communications, economics, social science, law, business management, or other relevant aspects which are beneficial to the operation of the CMO in accordance with the criteria and method as determined by the Committee.</p>	<p><i>Section 25:</i> There shall be a Committee Managing the Office of the National Cybersecurity Committee, abbreviated as "CMO," to supervise the general administration of the Office, consisting of the Minister of the Digital Economy and Society as the chairperson, Permanent Secretary of the Ministry of Digital Economy and Society, Director General of the Controller General's Department, the Secretary-General of the Civil Service Commission, the Secretary-General of the Office of the Public Sector Development, and honorary directors not exceeding six independent persons to be directors.</p> <p>The honorary directors under paragraph one shall be appointed by the Cabinet among the persons who have knowledge, expertise, and remarkable competency in Maintaining Cybersecurity, information technology and communications, economics, social science, law, business management, or other relevant aspects which are beneficial to the operation of the CMO in accordance with the publicly available and accessible criteria and method as determined by the Committee.</p> <p>This Committee shall perform its function of overseeing the management of the Office, which shall not replace any authority performing the function of tripartite agency.</p>
<p><i>Section 27:</i> The CMO shall have the following duties and powers:</p> <ol style="list-style-type: none"> (1) determine the management policy and approve the operational plan of the Office; (2) issue regulations regarding the organization, finance, human resources, general management, stock, internal inspection, and other support and welfare of the Office; (3) approve the payment plan and annual expense budget of the Office; (4) control the management and operation of the Office and Secretary-General in accordance with this Act and other relevant laws; (5) analyze the administrative order of the Secretary-General in relation to the management of the Office; (6) evaluate the result of the operation of the Office and the execution of the Secretary-General; (7) perform any other task as specified under this Act or other relevant laws as duties and powers of the CMO or as assigned by the Committee or the Cabinet. <p>In performing the duties under paragraph one, the CMO may appoint a sub-committee to consider,</p>	<p><i>Section 27:</i> The CMO shall have the following duties and powers:</p> <ol style="list-style-type: none"> (1) determine the management policy that is clear and precise and approve the operational plan of the Office; (2) issue regulations regarding the organization, finance, human resources, general management, stock, internal inspection, and other support and welfare of the Office, as well as penalty and fines to remedy violations by the Office; (3) approve the payment plan and annual expense budget of the Office in a transparent manner; (4) control the management and operation of the Office and Secretary-General in accordance with this Act and other relevant applicable domestic and international laws and policy including those that protect individual rights to freedom and privacy; (5) analyze the administrative order of the Secretary-General in relation to the management of the Office in a timely manner; (6) evaluate the result of the operation of the Office and the execution of the Secretary-General and utilizing this for the review of the policy and management of the Office;

<p>suggest, or perform any act as assigned by the CMO, with performance of such duties and meetings to be in accordance with the criteria and method determined by the CMO.</p> <p>The CMO may appoint the honorary committee who has expertise in aspects beneficial to the operation of the Office as a consultant of the CMO under the criteria and method determined by the Committee.</p>	<p>(7) perform any other task as specified under this Act or other relevant laws as duties and powers of the CMO or as assigned by the Committee or the Cabinet and subject to revision, which must be in line with international standards.</p> <p>In performing the duties under paragraph one, the CMO may appoint a qualified and publicly identified sub-committee to consider, suggest, or perform any act as assigned by the CMO, with performance of such duties and meetings to be in accordance with the comprehensive and accessible criteria and method determined by the CMO.</p> <p>The CMO may appoint the honorary committee who has expertise in aspects beneficial to the operation of the Office as a consultant of the CMO under the comprehensive, publicly available and accessible criteria and method determined by the Committee.</p>
<p><i>Section 30:</i> A Secretary-General shall have the following qualifications</p>	<p><i>Section 30:</i> A Secretary-General shall have the following qualifications determined following a transparent assessment</p>
<p><i>Section 31:</i> A person having any of the following characteristics shall be prohibited</p>	<p><i>Section 31:</i> A person having any of the following characteristics shall be prohibited, as determined following an independent and transparent assessment</p>
<p><i>Section 34:</i> Each year, there shall be a performance evaluation of a Secretary- General in accordance with the period and method determined by the Committee.</p>	<p><i>Section 34:</i> Each year, there shall be a performance evaluation of a Secretary- General in accordance with the clearly defined period and accessible method determined by the Committee.</p>
<p><i>Section 35:</i> Apart from the expiration of term, a Secretary-General vacates office upon:</p> <ol style="list-style-type: none"> (1) death; (2) resignation; (3) lacking qualifications as specified in section 30 or possessing prohibited characteristics as specified in section 31; (4) resolution for removal passed by the Committee on grounds of unsatisfactory or dishonest performance of duties, disgraceful behavior, or incapacity; (5) removal from the Committee based on failure to pass the performance evaluation; and (6) vacating in accordance with the terms specified under the employment agreement or agreement between the Committee and the Secretary-General. 	<p><i>Section 35:</i> Apart from the expiration of term, a Secretary-General vacates office upon:</p> <ol style="list-style-type: none"> (1) death; (2) resignation; (3) lacking qualifications as specified in section 30 or possessing prohibited characteristics as specified in section 31; (4) resolution for removal passed by the Committee on grounds of unsatisfactory or dishonest performance of duties, disgraceful behavior, or incapacity determined through specific criteria; (5) removal from the Committee based on failure to pass the performance evaluation that is conducted in a fair and transparent manner; and (6) voluntarily vacating in accordance with the terms specified under the employment agreement or agreement between the Committee and the Secretary-General.
<p><i>Section 36:</i> A Secretary-General under the supervision of the Committee, CRC, and CMO shall comply with the orders of the Committee, CRC, and CMO under the duties and powers as follows:</p>	<p><i>Section 36:</i> A Secretary-General under the supervision of the Committee, CRC, and CMO shall comply with the orders of the Committee, CRC, and CMO under the duties and powers as follows:</p>

- (1) manage the operation of the Office to accomplish in accordance with the mission of the Office, and with the policy and plan on Maintaining Cybersecurity, the operational plan for Maintaining Cybersecurity, the policies of the Cabinet and the Committee, and regulations, policies, resolutions and notifications of the CMO;
- (2) issue regulations under the policy of the Committee and CRC that are not contrary to the law, Cabinet resolutions, and the regulations, policies, resolutions, and notifications determined by the Committee and CRC;
- (3) be a supervisor of the officers and employees of the Office and evaluate the performances of officers and employees of the Office in accordance with the regulations of the CMO and the rules of the Office;
- (4) appoint the deputy Secretary-General or assistant of the Secretary-General as approved by the Committee to be an assistant in the operation of the Secretary- General as assigned by the Secretary-General;
- (5) assign, appoint, promote, demote, deduct the salaries or wages of, execute disciplinary action against officers and employees of the Office, and remove officers and employees of the Office in accordance with the regulations determined by the CMO and the rules of the Office;
- (6) perform any other task as specified under the regulations, policies, resolutions, or notifications of the CMO or the CRC.

- (1) manage the operation of the Office to accomplish in accordance with the mission of the Office, and with the [evidence-based](#) policy and plan on Maintaining Cybersecurity, the operational plan for Maintaining Cybersecurity, the policies of the Cabinet and the Committee, and regulations, policies, resolutions and notifications of the CMO;
- (2) issue regulations under the policy of the Committee and CRC that are not contrary to the law, Cabinet resolutions, and the [comprehensive, publicly available and accessible](#) regulations, policies, resolutions, and notifications determined by the Committee and CRC;
- (3) be a supervisor of the officers and employees of the Office and evaluate the performances of officers and employees of the Office in accordance with the regulations of the CMO and the rules of the Office;
- (4) appoint ~~the~~ a [qualified](#) deputy Secretary-General or assistant of the Secretary-General as approved by the Committee to be an assistant in the operation of the Secretary- General as assigned by the Secretary-General;
- (5) assign, appoint, promote, demote, deduct the salaries or wages of, execute disciplinary action against officers and employees of the Office, and remove officers and employees of the Office in accordance with the [comprehensive, publicly available and accessible](#) regulations determined by the CMO and the rules of the Office;
- (6) perform any other task as specified under the regulations, policies, resolutions, or notifications of the CMO or the CRC. [This may be subject to review by the tripartite agency or by competent grievance redressal mechanisms.](#)

Section 39: The Office shall prepare an annual report to be submitted to the Committee within one hundred and eighty days from the end of the fiscal year, and shall disclose the annual report to the public.

The annual report under paragraph one shall describe the details of balance sheets as approved by an auditor, the performance of the Office, and the outcome of the performance evaluation of the Office during the previous fiscal year.

The evaluation of the Office under paragraph two shall be done by an external person who has been approved by the CMO.

Section 39: The Office shall prepare an annual report to be submitted to the Committee within one hundred and eighty days from the end of the fiscal year, and shall disclose the annual report to the public.

The annual report under paragraph one shall describe the details of balance sheets as approved by an auditor, the performance of the Office, and the outcome of the performance evaluation of the Office during the previous fiscal year.

The evaluation of the Office under paragraph two shall be done by an external [independent and qualified](#) person who has been approved by the CMO.

<p><i>Section 41:</i> Maintaining Cybersecurity shall take into consideration the unity and integration of the operation of Government Agencies and private organizations, and shall align with the national policy and plan regarding the digital development for economy and society in accordance with the laws regarding the digital development for economy and society, and the policy and master plan which are related to maintaining the security of the National Security Council.</p> <p>The operation on Maintaining Cybersecurity shall aim to create the capability to prevent, cope with, and mitigate risks from Cyber Threats, especially in protecting the Critical Information Infrastructure of the country.</p>	<p><i>Section 41:</i> Maintaining Cybersecurity shall take into consideration the unity and integration as well as inclusivity and collaboration of the operation of Government Agencies and private organizations, and shall align with the national policy and plan regarding the digital development for economy and society in accordance with the laws regarding the digital development for economy and society, and the policy and master plan which are related to maintaining the security of the National Security Council.</p> <p>The operation on Maintaining Cybersecurity shall aim to create the capability to prevent, cope with address, and mitigate risks from Cyber Threats, especially in protecting the Critical Information Infrastructure of the country.</p>
<p><i>Section 42:</i> The policy and plan on Maintaining Cybersecurity shall at least contain the following objectives and approaches:</p> <ol style="list-style-type: none"> (1) integration of management in Maintaining Cybersecurity of the country; (2) establishment of measures and mechanisms to develop capability to prevent, cope with, and mitigate the risks from Cyber Threats; (3) establishment of measures to protect the Critical Information Infrastructure of the country; (4) cooperation between the public and private sector, and international cooperation for Maintaining Cybersecurity; (5) research and development of technology and knowledge related to Maintaining Cybersecurity; (6) development of personnel and experts in Maintaining Cybersecurity, both in the public and the private sector; (7) creation of awareness and knowledge in Maintaining Cybersecurity; (8) development of rules and laws for Maintaining Cybersecurity. 	<p><i>Section 42:</i> The policy and plan on Maintaining Cybersecurity shall at least contain the following objectives and approaches:</p> <ol style="list-style-type: none"> (1) integration of management in Maintaining Cybersecurity of the country; (2) establishment of measures and mechanisms to develop capability to prevent, cope with address, and mitigate the risks from Cyber Threats; (3) establishment of measures to protect the Critical Information Infrastructure of the country; (4) cooperation between the public and private sector, and international cooperation for Maintaining Cybersecurity; (5) research and development of technology and knowledge related to Maintaining Cybersecurity; (6) development of personnel and experts in Maintaining Cybersecurity, both in the public and the private sector; (7) creation of awareness and knowledge in Maintaining Cybersecurity including amongst civil society; (8) development of rules and laws for Maintaining Cybersecurity; and (9) Learning from and adapting to changing technology that could enhance or compromise cyber-capability.
<p><i>Section 43:</i> The Committee shall prepare a policy and plan for Maintaining Cybersecurity in accordance with section 42 to propose to the Cabinet for approval, which shall be published in the Government Gazette. Once published, Government Agencies, Supervising or Regulating Organizations, and Organizations of Critical Information Infrastructure as determined in the plan on Maintaining Cybersecurity shall take action to be in accordance with such policy and plan.</p> <p>In preparing the policy and plan under paragraph one, the Office shall hold a hearing or meeting with the</p>	<p><i>Section 43:</i> The Committee shall prepare a policy and plan for Maintaining Cybersecurity in accordance with section 42 to propose to the Cabinet and by all stakeholders to the process for approval, which shall be published in the Government Gazette. Once published, Government Agencies, Supervising or Regulating Organizations, and Organizations of Critical Information Infrastructure as determined in the plan on Maintaining Cybersecurity shall take action to be in accordance with such policy and plan, in so far as it does not violate or compel the violation of individual rights.</p>

<p>Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.</p>	<p>In preparing the policy and plan under paragraph one, the Office shall hold a hearing or meeting with the Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure, and with other stakeholders such as the private sector, technical experts and civil society.</p>
<p><i>Section 44:</i> The Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure shall prepare a Code of Practice and standard framework for Maintaining Cybersecurity of each organization in accordance with the policy and plan on Maintaining Cybersecurity without delay.</p> <p>The Code of Practice for Maintaining Cybersecurity under paragraph one, at least, shall consist of the following:</p> <ul style="list-style-type: none"> the plan for examining and assessing risks related to Maintaining Cybersecurity by an examiner, internal auditor, or independent external auditor, at least once per year; the plan for coping with Cyber Threats. <p>For the benefit of preparing the Code of Practice for Maintaining Cybersecurity in paragraph one, the Office, upon the approval of the Committee, shall prepare a Code of Practice and standard framework for the Government Agency, Supervising or Regulating Organization, or Organization of Critical Information Infrastructure to use as a guideline to prepare or exercise as a Code of Practice of the Government Agency, Supervising or Regulating Organization, or Organization of Critical Information Infrastructure. In case such organizations do not yet have or have but incomplete or is not in accordance with the Code of Practice and standard framework, such Code of Practice and standard framework shall be enforced.</p>	<p><i>Section 44:</i> The Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure shall prepare a Code of Practice and standard framework for Maintaining Cybersecurity of each organization in accordance with the policy and plan on Maintaining Cybersecurity without delay, and to the extent that they comply with other relevant domestic laws and international legislations or standards.</p> <p>The Code of Practice for Maintaining Cybersecurity under paragraph one, at least, shall consist of the following:</p> <ul style="list-style-type: none"> the plan for examining and assessing risks related to Maintaining Cybersecurity by an examiner, internal auditor, or independent external auditor, in a uniform and transparent manner at least once per year; the plan for coping with Cyber Threats that does not harm the protection of individual rights. <p>For the benefit of preparing the Code of Practice for Maintaining Cybersecurity in paragraph one, the Office, upon the approval of the Committee, shall prepare a Code of Practice and standard framework for the Government Agency, Supervising or Regulating Organization, or Organization of Critical Information Infrastructure to use as a guideline to prepare or exercise as a Code of Practice of the Government Agency, Supervising or Regulating Organization, or Organization of Critical Information Infrastructure. In case such organizations do not yet have or have but incomplete or is not in accordance with the Code of Practice and standard framework, such Code of Practice and standard framework shall be enforced following a periodic review and assessment to improve their practices.</p>
<p><i>Section 45:</i> The Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure have a duty to prevent, cope with, and mitigate risks from Cyber Threats in accordance with the Code of Practice and standard framework for Maintaining Cybersecurity of each organization and shall act in order to be in compliance with the Code of Practice and standard framework for Maintaining Cybersecurity in accordance with section 13 paragraph one (4).</p>	<p><i>Section 45:</i> The Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure have a duty to prevent, cope with address, and mitigate risks from Cyber Threats in accordance with the Code of Practice and standard framework for Maintaining Cybersecurity of each organization and shall act in order to be in compliance with the Code of Practice and standard framework for Maintaining Cybersecurity in accordance with section 13 paragraph one (4); in situations where there is evidence to believe that there may be a risk of serious harm.</p>

<p><i>Section 46:</i> For the benefit of Maintaining Cybersecurity, the Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure shall notify the name of executive officials and operational officials for the coordination of Maintaining Cybersecurity to the Office.</p>	<p><i>Section 46:</i> For the benefit of Maintaining Cybersecurity, the Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure shall notify the name of executive officials and operational officials for the coordination of Maintaining Cybersecurity to the Office.</p>
<p><i>Section 47:</i> In case the performance of the duties in accordance with this Act requires knowledge and expertise, the Committee or the CRC may assign the Secretary-General to hire an expert as appropriate for each specific task.</p> <p>The expert in paragraph one shall have appropriate qualifications or experience in accordance with the notification prescribed by the Committee.</p>	<p><i>Section 47:</i> In case the performance of the duties in accordance with this Act requires knowledge and expertise, the Committee or the CRC may assign the Secretary-General to hire an expert as appropriate for each specific task.</p> <p>The expert in paragraph one shall have appropriate qualifications or experience in accordance with the notification prescribed by the Committee, with a transparent selection process.</p>
	<p><i>Section 84:</i> The tripartite agency shall be responsible for auditing through continuous semi-annual or annual monitoring and evaluation of the progress and efficiency of implementation of the Act. This shall be done by setting out indicators to analyze the performance of the Act, to address its ability to meet the needs and set out responsibilities of all stakeholders. The report produced using these key metrics shall be submitted to the Council of Ministers, the Committee and made available to the general public. This input may be used to review the National Cybersecurity Act of Thailand after a period of time, to integrate development in technology, change in cyberattacks and violation of rights as a result.</p>



5.4.1. Context

The National Cybersecurity Act as discussed above provides extensive power to the NCSC, CRC, the Office of the National Cybersecurity Committee, the CMO, as well as to supervising and regulatory bodies that are involved in the protection of the digital space through identification, protection and mitigation of cybersecurity threats. This extensive power also extends to control over CIIs. This power allows the bodies and agencies under the Act to apply their discretion as they choose to. CIIs would need to have something to offer the control authorities to leverage their power and regain control. CIIs in turn could also try to exercise control over the general public, which could require leveraging in return. This interplay of power and wrestling for control could lead to dubious circumstances, that would worsen the lack of transparency.



“Critical infrastructure needs to be clearly defined in order for cybersecurity legislations to be effective. In the National Cybersecurity Act of Thailand, the NCSC can add ‘anything’ to critical infrastructure, which is dangerous and will negatively influence businesses’ decisions to operate in the country. To overcome this issue, broad definitions included in the Act need to be addressed with focus placed on security outcomes, balanced with transparency.”

Jeff Paine,
Managing Director,
Asia Internet Coalition (AIC)

a. Identification of Critical Information Infrastructure (CII)

As discussed under Challenge 1, Sections 3, 48 and 49 of the Act have left the definition of CIIs open to interpretation. Section 49 has identified CIIs as those that contribute to (1) national security; (2) substantive public service; (3) banking and finance; (4) Information technology and telecommunications; (5) transportation and logistics; (6) energy and public utilities; and (7) public health. It also provides that other organizations can be identified as CIIs as deemed necessary by the NCSC. In this respect, the NCSC must announce and publish in the Government Gazette, a set of rules for the identification of CIIs. However, there is no solution provided in case the rules prove to give authorities excessive control and the only oversight can be exercised by the Cabinet, who may not express any objection to a guideline drafted by a Committee that is Chaired by the Prime Minister, who has probably assigned them their position to start with. In such circumstances, the NCSC will have the freedom to identify any organization or types of organizations as CIIs. For example, if a political regime considers all digital media could threaten their position of power and thus ‘social order’, they could easily provide criteria that identifies all digital media organizations as CII. Such a move will further threaten online freedom and the civic space, and all CIIs that fall under the category of ‘digital media organizations’ would either practice self-censorship to protect their existence, make themselves ‘useful’ to the government authorities or have to face their ire.

b. Reporting obligations of CIIs, with respect to cybersecurity incidents

CIIs, such as government agencies and organizations of CIIs face a difficult challenge with respect to cybersecurity incident responses, particularly private entities. Government agencies would most likely have different standards applied to them, as compared to the private sector. The main difficulty is excessive government intrusion in the form of reporting cybersecurity threats to authorities under Sections 54, 55, 57, 73 and 74 of the Act, with CIIs having to report all threats. It is often difficult for the private sector to monitor and constantly report all threats, with the nature of threats changing and the information to be shared sometimes being confidential. Sometimes it is also impossible to determine if something is a threat, until a cyberattack has taken place. Over-reporting in the absence of a proven risk could lead to private sector enterprises not taking appropriate action when ‘a real risk of harm’ exists. If a risk assessment report submitted by organizations or individuals is not proper it may also have to be compiled and submitted again. **Failure to report or submit risk assessment reports could result in imprisonment and heavy penalty, according to Sections 73 and 74 of the Act. In this situation, with government authorities having the upper hand, it would be easy for private sector enterprises to make a wrong decision to compromise the privacy and human rights of individuals if asked to; or by passing on the burden to individuals they provide a service to, such as in the case of financial institutions that could overcharge for services. Collaboratively tackling cybersecurity threats with all stakeholders, rather than over broad reporting obligations with strict government oversight could remove the difficult atmosphere this would create, particularly for the private sector.**

This is a clear cyclical situation where controlling authorities could use their discretion to exert power over CIIs, until the CII can offer the control authority something to regain power; and CIIs could leverage and hold their authority over the public.

5.4.2. Recommended Amendments

Original Text (in sequential order)	Suggested Changes , Deletions and Additions to the National Cybersecurity Act
<p><i>Section 48:</i> The Critical Information Infrastructure is an operation which are important to national security, military security, economic security, and public order in the country, and it shall be the duty of the Office to assist and provide assistance to prevent, cope with, and mitigate risks from Cyber Threats, especially, Cyber Threats that affect or occur in relation to the Critical Information Infrastructure.</p>	<p><i>Section 48:</i> The Critical Information Infrastructure is an operation which are is important to national security, military security, economic security, individual security, privacy and public order in the country, and it shall be the duty of the Office to assist and provide assistance to prevent, cope with address, and mitigate risks from Cyber Threats, especially, Cyber Threats that affect or occur in relation to the Critical Information Infrastructure.</p>
<p><i>Section 49:</i> The Committee shall have the power to prescribe in a notification the characteristics of the organizations that have a mission or provide services in the following aspects, as an Organization of Critical Information Infrastructure:</p> <ol style="list-style-type: none"> (1) national security; (2) substantive public service; (3) banking and finance; (4) Information technology and telecommunications; (5) transportation and logistics; (6) energy and public utilities; (7) public health; 	<p><i>Section 49:</i> The Committee shall have the power to prescribe in a notification prior to implementation of this Act the clearly identifiable characteristics of the organizations that have a mission or provide services in the following aspects, as an Organization of Critical Information Infrastructure:</p> <ol style="list-style-type: none"> (1) national security; (2) substantive public service; (3) banking and finance; (4) Information technology and telecommunications; (5) transportation and logistics; (6) energy and public utilities;

<p>(8) others as prescribed by the Committee.</p> <p>The consideration for the prescription of such mission or services under paragraph one shall be in accordance with the rules prescribed by the Committee, which shall be published in the Government Gazette. The Committee shall consider and review such prescription of the mission or services on a case-by-case basis as appropriate.</p>	<p>(7) public health; (8) others as prescribed by the Committee based on their criticality and as agreed upon by other stakeholders in the process.</p> <p>The consideration for the prescription of such mission or services under paragraph one shall be in accordance with the rules prescribed by the Committee, which shall be published in the Government Gazette. The Committee shall consider and review such prescription of the mission or services on a case-by-case basis as appropriate. This identification shall also be subject to periodic review by the tripartite agency or a public-private collaboration established specifically for Critical Information Infrastructure Protection (CIIP).</p>
<p><i>Section 50:</i> The Committee has the power to prescribe the characteristics, duties, and responsibilities of the coordinating agency for maintaining the security of computer systems for the Organization of Critical Information Infrastructure of section 49 to coordinate, monitor, cope with, and resolve Cyber Threats by prescribing the Government Agency that is ready or such Critical Information Infrastructure Supervising or Regulating Organization to perform such duties for the Organization of Critical Information Infrastructure in accordance with section 49, in whole or in part.</p> <p>Consideration for the prescription of such mission or services under paragraph one shall be in accordance with the rules prescribed by the Committee, which shall be published in the Government Gazette. The Committee shall consider and review such prescription of the mission or services on a case-by-case basis as appropriate.</p>	<p><i>Section 50:</i> The Committee has the power to prescribe the characteristics, duties, and responsibilities of the coordinating agency for maintaining the security of computer systems for the Organization of Critical Information Infrastructure of section 49 to coordinate, monitor, cope with address, and resolve Cyber Threats by prescribing the Government Agency that is ready or such Critical Information Infrastructure Supervising or Regulating Organization to perform such duties for the Organization of Critical Information Infrastructure in accordance with section 49, in whole or in part.</p> <p>Consideration for the prescription of such mission or services under paragraph one shall be in accordance with the rules prescribed by the Committee, which shall be published in the Government Gazette. The Committee shall consider and review such prescription of the mission or services on a case-by-case basis as appropriate, while seeking the input of other stakeholders affected by this decision.</p>
<p><i>Section 51:</i> In the event of any inquiries or claims related to the characteristics of the organizations having the mission or providing the services as prescribed in accordance with section 49 or section 50, the Committee shall make the final decision.</p>	<p><i>Section 51:</i> In the event of any inquiries or claims related to the characteristics of the organizations having the mission or providing the services as prescribed in accordance with section 49 or section 50, the Committee shall make the final decision or a solution may be sought from an effective grievance redressal process as agreed upon by those involved.</p>
<p><i>Section 52:</i> For the benefit of coordination, the Organization of Critical Information Infrastructure shall notify the name and contact information of the owner, the person possessing the computer, and the person monitoring the computer system to the Office, its Supervising or Regulating Organization, and the organization under section 50, within thirty days from the date the Committee prescribes the notification in accordance with section 49 paragraph two and section 50 paragraph two, or from the date the Committee</p>	<p><i>Section 52:</i> For the benefit of coordination, the Organization of Critical Information Infrastructure shall notify the name and contact information of the owner, the person possessing the computer, and the person monitoring the computer system to the Office, its Supervising or Regulating Organization, and the organization under section 50, within thirty days from the date the Committee prescribes the notification in accordance with section 49 paragraph two and section 50 paragraph two, or from the date the</p>

<p>issues a final judgement in accordance with section 51, as the case may be; the owner, the person possessing the computer, and the person monitoring the computer system shall at least be a person responsible for the management of such Organization of Critical Information Infrastructure.</p>	<p>Committee issues a final judgement in accordance with section 51, as the case may be; the owner, the person possessing the computer, and the person monitoring the computer system shall at least be a person responsible for the management of such Organization of Critical Information Infrastructure.</p>
<p><i>Section 53:</i> In the operation of Maintaining Cybersecurity of the Organization of Critical Information Infrastructure, the Supervising or Regulating Organization shall examine the minimum cybersecurity standard of the Organization of Critical Information Infrastructure under its supervision. If found that Organization of Critical Information Infrastructure does not comply with the standards, the Supervising or Regulating Organization shall notify the Organization of Critical Information Infrastructure which is below the standards to make correction in order to meet the standards without delay. If such Organization of Critical Information Infrastructure neglects or fails to comply within the period prescribed by the Supervising or Regulating Organization, the Supervising or Regulating Organization shall notify the CRC for consideration without delay.</p> <p>Upon receipt of notification under paragraph one, if the CRC considers and views that there is such reason and which may cause a Cyber Threat, the CRC may perform the following:</p> <ol style="list-style-type: none"> (1) in case of a Government Agency, the CRC shall notify the chief executive of the agency to exercise executive power to issue an order to the Government Agency or the Organization of Critical Information Infrastructure to correct and comply with the standards without delay; (2) in case of a private organization, the CRC shall notify the chief executive of the organization, the person possessing the computer, and the person monitoring the computer system of the Organization of Critical Information Infrastructure to make correction and comply with the standards without delay. 	<p><i>Section 53:</i> In the operation of Maintaining Cybersecurity of the Organization of Critical Information Infrastructure, the Supervising or Regulating Organization shall examine the minimum cybersecurity standard of the Organization of Critical Information Infrastructure under its supervision. If found that Organization of Critical Information Infrastructure does not comply with the standards, the Supervising or Regulating Organization shall notify the Organization of Critical Information Infrastructure which is below the standards to make correction in order to meet the standards without delay. If such Organization of Critical Information Infrastructure neglects or fails to comply within the period prescribed by the Supervising or Regulating Organization, the Supervising or Regulating Organization shall notify the CRC followed by an explanation for such a failure, for consideration without delay.</p> <p>Upon receipt of notification under paragraph one, if the CRC considers and views that there is such reason and which may cause a Cyber Threat that are highly imminent with material proof of the same particularly in situations where there is a reason to believe that there may be a risk of serious harm, the CRC may perform the following:</p> <ol style="list-style-type: none"> (1) in case of a Government Agency, the CRC shall notify the chief executive of the agency to exercise executive power to issue an order to the Government Agency or the Organization of Critical Information Infrastructure to correct and comply with the standards without delay; (2) in case of a private organization, the CRC shall notify the chief executive of the organization, the person possessing the computer, and the person monitoring the computer system of the Organization of Critical Information Infrastructure to make correction and comply with the standards without delay.
<p><i>Section 54:</i> The Organization of Critical Information Infrastructure shall conduct risk assessment on Maintaining Cybersecurity by having an examiner, including examination in the cybersecurity aspect by the information security auditor, internal auditor or external independent auditor, at least once per year.</p> <p>The Organization of Critical Information Infrastructure shall submit a summary report of the operation result</p>	<p><i>Section 54:</i> The Organization of Critical Information Infrastructure shall conduct risk assessment based on evidence obtained on Maintaining Cybersecurity by having an examiner, including examination in the cybersecurity aspect by the information security auditor, internal auditor or external independent auditor, at least once per year, in accordance with international standards in this respect particularly in situations where there is a reason to believe that there may be a risk of serious harm.</p>

<p>to the Office within thirty days after the operation has been finished.</p>	<p>The Organization of Critical Information Infrastructure shall submit a summary report of the operation result to the Office within thirty days after the operation has been finished, with appropriate steps taken to protect the identify of users and their rights as well as the integrity of their information systems.</p>
<p><i>Section 55:</i> In case the CRC views that the risk assessment on Maintaining Cybersecurity or the examination in the cybersecurity aspect in accordance with section 54 is not in compliance with the standards according to the report of the Supervising or Regulating Organization, the CRC shall order the Organization of Critical Information Infrastructure to conduct the risk assessment again to be in accordance with the standards, or proceed with the examination in other aspects that may affect the Critical Information Infrastructure.</p> <p>In case the Organization of Critical Information Infrastructure has already conducted the risk assessment on Maintaining Cybersecurity or examination in the cybersecurity aspect of paragraph one but the CRC views that it is not in compliance with the standards, CRC may perform the following:</p> <ol style="list-style-type: none"> (1) in case of a Government Agency, the CRC shall notify the chief executive of the agency to exercise executive power to issue an order to the Government Agency or Organization of Critical Information Infrastructure to correct and comply with the standards without delay; (2) in case of a private organization, the CRC shall notify the chief executive of the organization, the person possessing the computer, and the person monitoring the computer system of the Organization of Critical Information Infrastructure to make correction and comply with the standards without delay. <p>The Secretary-General shall monitor to ensure compliance of paragraph two.</p>	<p><i>Section 55:</i> In case the CRC views that the risk assessment on Maintaining Cybersecurity or the examination in the cybersecurity aspect in accordance with section 54 is not in compliance with the standards according to the report of the Supervising or Regulating Organization, the CRC shall order encourage the Organization of Critical Information Infrastructure to proactively conduct the risk assessment again to be in accordance with the standards, or proceed with the examination in other aspects that may affect the Critical Information Infrastructure.</p> <p>In case the Organization of Critical Information Infrastructure has already conducted the risk assessment on Maintaining Cybersecurity or examination in the cybersecurity aspect of paragraph one but the CRC views that it is not in compliance with the standards and the criteria of fairness in terms of procedure and content, CRC may perform the following:</p> <ol style="list-style-type: none"> (1) in case of a Government Agency, the CRC shall notify the chief executive of the agency to exercise executive power to issue an order to the Government Agency or Organization of Critical Information Infrastructure to correct and comply with the standards without delay; (2) in case of a private organization, the CRC shall notify the chief executive of the organization, the person possessing the computer, and the person monitoring the computer system of the Organization of Critical Information Infrastructure to make correction and comply with the standards without delay. <p>The Secretary-General shall monitor to ensure compliance of paragraph two.</p>

<p><i>Section 56:</i> The Organization of Critical Information Infrastructure shall establish a mechanism or process to monitor Cyber Threats or Cybersecurity Incidents which relates to its Critical Information Infrastructure in accordance with the standards as determined by the Supervising or Regulating Organization and in accordance with Code of Practice, including the system of Cybersecurity Solution as determined by the Committee or the CRC, and shall participate in the assessment on the readiness in coping with Cyber Threats as held by the Office.</p>	<p><i>Section 56:</i> The Organization of Critical Information Infrastructure shall establish a mechanism or process to monitor Cyber Threats or Cybersecurity Incidents which relates to its Critical Information Infrastructure in accordance with the publicly available and accessible standards as determined by the Supervising or Regulating Organization and in accordance with the publicly available and accessible Code of Practice, including the system of Cybersecurity Solution as determined by the Committee or the CRC, and shall participate in the assessment on the readiness in coping with Cyber Threats as held by the Office, unless they result in the violation of rights and public interest.</p>
<p><i>Section 57:</i> In the event of a Cyber Threat significantly occurring to the system of the Organization of Critical Information Infrastructure, the Organization of Critical Information Infrastructure shall report to the Office and the Supervising or Regulating Organization and cope with the Cyber Threats as prescribed in Part 4, the CRC may prescribe criteria and method of the reporting.</p>	<p><i>Section 57:</i> In the event of a Cyber Threat significantly occurring to the system of the Organization of Critical Information Infrastructure, the Organization of Critical Information Infrastructure shall report to the Office and the Supervising or Regulating Organization and cope with address the Cyber Threats as prescribed in Part 4, the CRC may prescribe criteria and method of the reporting, to which these critical information infrastructure organizations must also contribute.</p>



5.5.1. Context



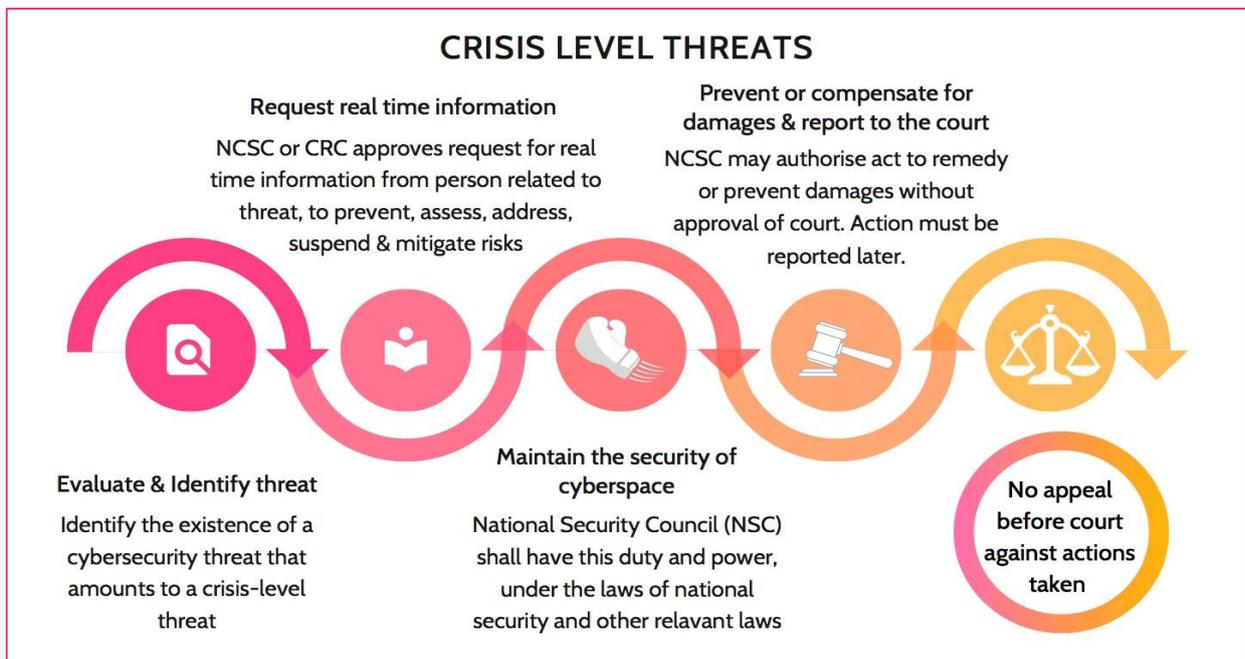
“Any limitation placed on individuals must be strictly provided by law, following the International Principles on the Application of Human Rights to Communications Surveillance. Mechanisms must be put in place to promote and ensure transparency on these aspects and accountability of the government in order to avoid oppressive state behaviour and misuse of legislations.”

Naman M. Aggarwal,
Asia Pacific Policy Counsel, Access Now

In the National Cybersecurity Act, there is a very clear lack of strong checks and balances or in some cases they are absent altogether. In the case of non-critical and critical cybersecurity threats, a Court order is required before any action is taken as provided under Section 65 of the Act. While the access to checks and balance through the Court system is limited for non-critical level cybersecurity incidents, it is completely absent and glaringly so in the case of critical level and crisis level cybersecurity threats. For understanding this better, however, we shall have a look to crisis level cybersecurity threats and the gaps in checks and balances with respect to them.

a. Crisis-level cybersecurity threats and the absence of checks and balances

In the case of crisis level cybersecurity incidents, checks and balances are already absent throughout the process when it comes to accountability and transparency. This is seen as follows: (a) not providing clear criteria for identifying the existence of threats that may cause damage under Section 60 as crisis-level threats, without any proof required on evidence of it causing harm and without limiting action based on necessity to meet a legitimate aim or for it to be a proportionate response in terms of the threat faced; (b) not receiving the input of all stakeholders that could be affected, in the drafting of policy, strategies and guidelines, as well as in identification of threats or any other decision-making processes, an aspect which is restricted to very powerful authorities that are the only ones allowed to determine the existence of a crisis-level threat; (c) not having a credible or independent monitoring or oversight mechanism; (d) maintaining security of cyberspace by using national security related laws with the NCSC having authority following Section 67 of the Act, which by its nature will always prioritize security over the rights of individuals; and (e) not encouraging transparency in the form of publicly available and accessible implementation reports.



b. Crisis-level cybersecurity threats and the use of the Court system

“What must be understood is that even though a Court order is required in certain circumstances under the National Cybersecurity Act, more attention will be given to security than to peoples’ rights. Also, a person who is questioned may often be unable to defend himself or herself; and they have no other choice but to obey orders given by the Committees established under the Act.”

Kanathip Thongraweewong,
Director of Digital Media Law Institution
and Associate Professor,
Kasem Bundit University

Lack of accountability in terms of decision-making and in other aspects makes it important to think about checks and balances through the Court system. The Court system cannot be used to appeal at all with respect to crisis-level cybersecurity threats as provided in Section 69, by those who are ordered to respond to these threats. However, there is solely one area where the connection with the Court system remains, however tenuous. This is in reporting to the Court under Section 68 of the Act when action is taken to prevent or remedy damages caused by critical-level cybersecurity threats. This information is submitted as a notification of the operations to a Competent Court without delay. Individuals do not have a choice but to cooperate. This is following an order by the NCSC, assigning the power to act and to bypass a motion to the Court, prior to taking action. This is worsened by the fact that nowhere in the Act is there any information on what type of action could be taken in response to crisis-level cybersecurity threats at all.

5.5.2. Recommended Amendments

Original Text (in sequential order)	Suggested Changes , Deletions and Additions to the National Cybersecurity Act
<p><i>Section 67:</i> In case there is a Cyber Threat at a crisis level, it shall be in the duty and power of the National Security Council in Maintaining Cybersecurity under the laws on National Security Council and other relevant laws.</p>	<p><i>Section 67:</i> In case there is a Cyber Threat at a crisis level, it shall be in the duty and power of the National Security Council in Maintaining Cybersecurity under the laws on National Security Council and other relevant laws, without compelling the violation of individual rights and the sharing of personal data.</p>
<p><i>Section 68:</i> In case it is urgent and necessary and the Cyber Threat is at a crisis level, the Committee may assign to the Secretary-General the power to act, only to the extent it is necessary to prevent and remedy the damages in advance, and the motion to the Court is not required to be submitted. However, after such operations, the details of the operations shall be notified to the Competent Court without delay.</p> <p>In a critical or crisis case, for the benefit of preventing, assessing, coping with, suppressing, suspending, and mitigating the risks from the Cyber Threat, the Secretary-General, upon the approval of the Committee or CRC, shall have the power to request real-time information from a person related to the Cyber Threat. Such person shall cooperate with and facilitate the Committee or the CRC without delay.</p>	<p><i>Section 68:</i> In case it is urgent and necessary and the Cyber Threat is at a crisis level, the Committee may assign to the Secretary-General the power to act requirement to seek court permission to identify crisis cybersecurity threats supported by evidence to believe that there may be a risk of serious harm and only to the extent it is necessary to prevent and remedy the damages in advance, and the motion to the Court is not required to be submitted.</p> <p>An independent, impartial and competent judicial authority such as a special court established under this Act or through an ombudsperson or a multi-stakeholder tripartite agency, will determine the appropriateness of action taken to be necessary and proportionate to protect a legitimate aim, its extent, the resulting damages, and the reimbursement provided. This information must also be made available to the general public. However, after such operations, the details of the operations shall be notified to the Competent Court without delay.</p> <p>In a critical or crisis case, for the benefit of preventing, assessing, coping with addressing, suppressing, suspending, and mitigating the risks from the Cyber Threat, the Secretary-General, upon the approval of the Committee or CRC, shall have the power to request real-time information from a person related to the Cyber Threat, as necessary, proportionate and to the extent required to address the threat. Such person shall cooperate with and facilitate the Committee or the CRC without delay.</p>
<p><i>Section 69:</i> A person receiving an order related to coping with a Cyber Threat may only appeal such order for Cyber Threats at a non-critical level.</p>	<p><i>Section 69:</i> A person receiving an order related to coping with addressing a Cyber Threat may only appeal such order for Cyber Threats at a non-critical level and a crisis level, before a court or other grievance redressal mechanisms prior to the resolution of the threat. In the case of a critical or crisis-level threats, individuals may appeal the situation once the threat has been addressed before an independent, impartial and competent judicial authority such as a specialized court established under this Act or through an ombudsperson.</p>



5.6.1. Context



“The flaw in the National Cybersecurity Act of Thailand remains that those who drafted the final text adopted into law are also the ones who will be enforcing it, which resulted in them providing more authority and power to themselves. Laws instead need to be drafted by experts or stakeholders who will be impacted by the law, rather than by enforcers.”

Dr. Bhume Bhumiratana,
Advisor, National Cybersecurity Committee
(Interim)

Government authorities and their representatives under the National Cybersecurity Act have remedies against public sector and private sector organizations, as well as against individuals responsible for the violation of this Act by compelling them to give information, by impounding computers, and by criminalization which could lead to fines and imprisonment, according to Sections 72, 73, 74, 75, and 76 of the Act. However, the Act does not provide for any remedy against these authorities that can violate rights of organizations and individuals, when unchecked allowing for lack of accountability and complete impunity.

a. Failure to provide effective remedy

This Act fails to provide effective remedy in two types of cases. These are:

1. **Remedy against officers and individuals for violation of this Act:** In this situation, wherein officers and individuals are responsible for negligently, unlawfully or otherwise revealing information gathered respectively under Sections 70, 71 and 72 of the Act. Here those affected do not have the opportunity to seek redress against the fixed criminal penalty and fine at all, least of all through an accessible and effective grievance redressal mechanism in order to seek fair treatment and just compensation, based on the amount of damage caused and to avoid recurrence.
2. **Remedy for individuals and organization of CII that are facing penalty due to violation or failure to comply with the Act:** Under Sections 73, 74, 75 and 76; individuals and organization of CII that fails to report a threat, fails to comply with a summoning letter, or violates or fails to comply with an order of the CRC on responses to critical level threats under Sections 65 and 66 face criminal sentences as well as fines under this Act. The only protection against such strict charges is if the individuals or organization of CII can provide ‘reasonable cause’. However, this has not been defined in the Act which leaves another aspect to the discretion of implementing authorities under the Act. For the provision

of an appropriate remedy, it must consider reasonable information that is 'sufficient to establish inability to carry out an action.' Moreover, reasonable time and opportunity must be given to clarify reasons especially if failure to comply is unintentional or connected with technical limitations.

b. Stopping access to remedy

As explained under Challenge 5, access to remedy in the form of appeal is specifically prohibited in the case of critical level and crisis level cybersecurity threats, according to Section 69 of the Act. Since the decision on whether a cybersecurity threat is at crisis-level is only up to government authorities, so not allowing for a remedy against the decision identifying the threat would be doubly unfair. In this case, such a decision should be reached following the input of an independent, impartial and competent authority or through the support of an ombudsperson. This situation may also be monitored by a multi-stakeholder agency solely fulfilling this role.

c. Further violation of rights, while barring access to remedy

This Act fails to provide remedy, bars or stops those affected from accessing remedy while also violating individual rights further.

This violation of rights exists with respect to two provisions of the Act:

1. **Section 70, which prohibits the disclosure or sending of computer data, computer traffic data or other data related to the users that is required to assess a cybersecurity threat.** In this case, it fails to provide instructions on how the information must be handled to safeguard it appropriately and effectively. Neither does it require to notify users of their information being accessed and retained by the authorities.

Furthermore, it does not allow for any penalty, if this information will benefit a lawsuit against a person who violates not just the National Cybersecurity Act but also other Acts. This could allow for the misuse of this power to collect information, which could subsequently be wrongly used to charge individuals for other crimes such as libel, defamation, slander to benefit the government authorities. Penalties do not apply even where this would benefit a case on misuse of power by authorities. This could also lead to misuse of the information gathered and retained for the purpose of charging an official. Thus, protection must be guaranteed by strictly limiting the damage to an individual or entity, who could be impacted by the misuse of the information accessed and gathered.

2. **Section 77, which holds directors or manager or any person responsible for acts or omissions resulting from their orders that has resulted in an offense by a juristic person.** This penalty is unfair to private individuals who are held responsible for Acts that could be committed by an organization, even if their order could result in a violation further down the command chain. Moreover, there is no opportunity provided to these individuals to explain the situation or to seek remedy where appropriate and necessary. This provision must be struck down in its entirety.

5.6.2. Recommended Amendments

Original Text (in sequential order)	Suggested Changes , Deletions and Additions to the National Cybersecurity Act
<p><i>Section 70:</i> The officers under this Act shall not disclose or send computer data, computer traffic data, other data related to the computer system, or data of the users obtained from this Act to any person. Any officer violating shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both.</p> <p>Paragraph one shall not apply to act for the benefit of litigation against an offender under this Act or an offender under other laws or for the benefit of the litigation against the officer related to the exercising of unlawful authority.</p>	<p><i>Section 70:</i> The officers under this Act shall not disclose or send computer data, computer traffic data, other data related to the computer system, or data of the users obtained from this Act to any person, as well as in the case of privileged information or that which would be inconsistent with protecting intellectual property rights or trade secrets. In this respect, restrictions shall be placed on the handling of such information to appropriate and effectively safeguard it, and should be accompanied by notifications to third parties and individuals that will be affected. Any officer violating shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both.</p> <p>Paragraph one shall not apply to act for the benefit of litigation against an offender under this Act or an offender under other laws or for the benefit of the litigation against the officer related to the exercising of unlawful authority. However, even in such a case effort must be made to limit the damage to an individual or entity that could be negatively impacted by such an action.</p>
<p><i>Section 71:</i> Any officer under this Act negligently causing other persons to know computer data, computer traffic data, data of the users, or other data related to the computer system obtained from this Act, shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both.</p>	<p><i>Section 71:</i> Any officer under this Act negligently causing other persons to know computer data, computer traffic data, data of the users, or other data related to the computer system obtained from this Act, shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both. Additionally, those affected may seek redress against such officials through an accessible and effective grievance redressal mechanism in order to seek fair treatment and just compensation based on the amount of damage caused, and in order to avoid its recurrence.</p>
<p><i>Section 72:</i> Any person who knows computer data, computer traffic data, data of the users, or data related to the computer system that the officer has obtained from this Act and unlawfully discloses such data to any person shall be subject to imprisonment not exceeding two years, a fine not exceeding Baht forty thousand, or both.</p>	<p><i>Section 72:</i> Any person who knows computer data, computer traffic data, data of the users, or data related to the computer system that the officer has obtained from this Act and unlawfully discloses such data to any person shall be subject to imprisonment not exceeding two years, a fine not exceeding Baht forty thousand, or both. Those affected may seek redress against such individuals through any accessible and effective grievance redressal mechanism in order to seek fair treatment and just compensation based on the amount of damage caused, and in order to avoid its recurrence.</p>

<p><i>Section 73:</i> Any Organization of Critical Information Infrastructure not reporting a Cyber Threat incident in accordance with section 57 without reasonable cause shall be subject to a fine not exceeding Baht two hundred thousand.</p>	<p><i>Section 73:</i> Any Organization of Critical Information Infrastructure not reporting a Cyber Threat incident in accordance with section 57 without reasonable cause that is sufficient to establish their inability to report, shall be subject to a fine not exceeding Baht two hundred thousand. Reasonable time and opportunity must be provided to clarify reasons for failure to report cybersecurity threats, which is essential particularly when failure to comply is unintentional or linked to technical constraints.</p>
<p><i>Section 74:</i> Any person not complying with the summoning letter of the Competent Officials, or not sending information to the Competent Official in accordance with section 62 (1) or (2) without a reasonable cause, as the case may be, shall be subject to a fine not exceeding Baht one hundred thousand.</p>	<p><i>Section 74:</i> Any person not complying with the summoning letter of the Competent Officials, or not sending information to the Competent Official in accordance with section 62 (1) or (2) without a reasonable cause that is sufficient to establish their inability to comply with summons or failure to send information, as the case may be, shall be subject to a fine not exceeding Baht one hundred thousand.</p> <p>Individuals who fail to submit a report as requested by officials under Section 62 (1) or (2), without any justified reasoning that is sufficient to establish their inability to report, may be subject to a fine of less than 100,000 Thai baht. Reasonable time and opportunity must be provided to clarify reasons for failure to report cybersecurity threats, which is essential particularly when failure to comply is unintentional or linked to technical constraints.</p>
<p><i>Section 75:</i> Any person violating or not complying with an order of the CRC in accordance with section 65 (1) (2) without a reasonable cause shall be subject to a fine not exceeding Baht three hundred thousand and a daily fine not exceeding Baht ten thousand from the date on which the CRC issues the orders until compliance.</p> <p>Any person violating or not complying with the order of the CRC in accordance with section 65 (3) and (4) or not complying with the court order in accordance with section 65 (5) shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both.</p>	<p><i>Section 75:</i> Any person violating or not complying with an order of the CRC in accordance with section 65 (1) (2) without a reasonable cause that is sufficient to establish their inability to comply with the order or reasons for its violation shall be subject to a fine not exceeding Baht three hundred thousand and a daily fine not exceeding Baht ten thousand from the date on which the CRC issues the orders until compliance.</p> <p>Any person violating or not complying with the order of the CRC in accordance with section 65 (3) and (4) or not complying with the court order in accordance with section 65 (5) shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both.</p> <p>Reasonable time and opportunity must be provided to clarify reasons for failure to report cybersecurity threats, which is essential particularly when failure to comply is unintentional or linked to technical constraints.</p>
<p><i>Section 76:</i> Any person disrupting or not complying with an orders of the CRC or the Competent Official performing its duty in accordance with the CRC's order in accordance with section 66 (1), or not</p>	<p><i>Section 76:</i> Any person disrupting or not complying with an orders of the CRC or the Competent Official performing its duty in accordance with the CRC's order in accordance with section 66 (1), or not complying</p>

<p>complying with the Court order in accordance with section 66 (2), (3), or (4), without a reasonable cause shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both.</p>	<p>with the Court order in accordance with section 66 (2), (3), or (4), without a reasonable cause that is sufficient to establish their inability to comply with the order or reasons for their disruption, shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both. Reasonable time and opportunity must be provided to clarify reasons for failure to report cybersecurity threats, which is essential particularly when failure to comply is unintentional or linked to technical constraints.</p>
<p><i>Section 77:</i> In case the person committing an offense under this Act is a juristic person, if such offense is a result of the order or the act of a director or a manager or any person responsible for the operation of such juristic person or in case such person has the duty to order or act and omit to order or act, causing the juristic person to commit an offense, such person shall be liable for the penalties prescribed for such offense.</p>	<p><i>Section 77:</i> In case the person committing an offense under this Act is a juristic person, if such offense is a result of the order or the act of a director or a manager or any person responsible for the operation of such juristic person or in case such person has the duty to order or act and omit to order or act, causing the juristic person to commit an offense, such person shall be liable the juristic person shall be liable for the penalties prescribed for such offense.</p>

6. CONCLUSION & RECOMMENDATIONS

This Study and its conclusive recommendations are intended to serve as a guidance for the government as well as Members of Parliament to use while moving forward and taking next steps on the National Cybersecurity Act. Therefore, towards creating a human centered digital ecosystem in Thailand and a National Cybersecurity Act that place individuals and their rights at the center, the following actions are proposed for each of the stakeholders that are involved in the processes and impacted by the content of this legislation.



“A guideline is required for safeguards and good implementation of the National Cybersecurity Act in Thailand, in line with international human rights standards that Thailand is committed to, so cybersecurity threats and cyberattacks are addressed without any misuse.”

Emilie Pradichit,
Founder & Director,
Manushya Foundation

6.1. Recommendations to the Government

- (1) Review the content of the Act in accordance with this Study, to address all shortcomings including provisions that are broad, that violate human rights, that provide unchecked power, and that fail to acknowledge accountability and transparency in line with international human rights standards such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).
- (2) Draft an implementation document to support the study by clarifying the scope of the Act and preventing uncertainty in implementation, including with a clear explanation of terms such as national security, martial security, economic security, public order with the provision of examples to explain its limits, based on principles of necessity and proportionality. In this, human security must be placed at the center of cybersecurity responses with particular attention being given to security concerns of individuals and their human rights concerns.
- (3) Ensure all bodies, authorities and agencies assigned official duties under the Act work in coordination, and only carry out those functions that they are assigned with no actions taken that prove to be a conflict of interest.

- (4) Provide training to competent officials and authorities under the Act that would assist in its implementation and regulation to provide an understanding of all aspects of the Act, cybersecurity and digital rights using examples of its application, and insight into global good practices.
- (5) Avoid taking any steps that place an extra burden on ICT organizations or that pressure the private sector to take steps themselves that unnecessarily or disproportionately interfere with the rights of individuals, whether through laws, policies, or extra-legal means.
- (6) Show consideration for the responsibility of service providers to respect the rights of individuals to online freedom and data privacy, by defining categories of information which are exempted from disclosure to which the confidentiality clause would apply. This can also be achieved by formalizing commitments to the responsibility to respect rights by the ICT sector, through national action plans that specifically address their policies and initiatives, in line with the UN Guiding Principles on Business and Human Rights (UNGPs).
- (7) Take all steps in a collaborative and inclusive manner, with contributions of all stakeholders for a fair and competent decision making as well as an efficient and effective implementation process.
- (8) Set up accessible and appropriate mechanisms, judicial and non-judicial; provide, among the remedies, fair treatment, just compensation or satisfaction, and the establishment of sufficient grounds to avoid its recurrence. Regular review of the mechanisms must be carried out.

6.2. Recommendations to Members of Parliament (MP)

- (1) Propose amendments to the National Cybersecurity Act before the National Legislative Assembly (NLA) in accordance with this Study, to address all shortcomings in line with international human rights standards such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR); and gather consensus among other MPs to ensure these amendments are adopted into the text of the Act.
- (2) Hold the government accountable by ensuring that the steps taken by government bodies and agencies under the Act are evaluated and analyzed on an individual as well as regular basis, applied only in cases where there is a risk of serious harm and cover both the enterprises in the public and private sector without discrimination; particularly when such a step could result in the violation of rights of individuals affected.
- (3) Build discussion and debate around cybersecurity, digital rights and protections with specific attention paid to the country context as well as good practices adopted regionally and internationally, with the general public actively involved in providing the grassroots perspective.

6.3. Recommendations to Businesses

- (1) Provide training to all stakeholders including implementing authorities, civil society and affected communities on the technical aspects of cybersecurity, and the technical steps to be taken in terms of prevention of cybersecurity threats and during the implementation of the Cybersecurity Act to ensure that all responses are in line with international human rights standards.
- (2) Undertake studies and regular assessments that provide clear indicators of cyberattacks and cybersecurity threats, which must be identified and evaluated on a regular basis, in order to efficiently deal with the evolving nature of attacks and technological developments as well as to limit the damage cause by cybersecurity attacks and the steps taken to address them.
- (3) Ensure the companies' terms of service and policies are uniform and comply with international standards on freedom of expression and protection of data privacy, which are reviewed regularly to

ensure all circumstances and situations that may arise have been addressed, while also addressing new legal, technological and societal developments, in line with the obligation to respect human rights under the UN Guiding Principles on Business and Human Rights (UNGPs).

- (4) Create a landing page that clearly explains in a simplified form, the rules, regulations and practices with respect to content restrictions, access to user data and other steps taken that could violate the rights of individuals to online freedom, privacy and guarantees of data protection.
- (5) Ensure that any requests, orders and commands to take down digital content or access information must be based on validly enacted law, subject to external and independent oversight, and demonstrates a necessary as well as proportionate means to achieve one or more aims.
- (6) Include notifications to third parties or private individuals, who may be affected by requests for information.
- (7) Provide users with an opportunity to challenge decisions, particularly on the take down of or access to their information when unlawful under national or international law; or if the restrictions are unfair and unduly restrictive.
- (8) Seek to prevent or mitigate the adverse impacts of the private sector's involvement, to the maximum extent allowed by law, by taking all necessary and lawful measures to ensure that they do not cause, contribute or become complicit in rights abuses.
- (9) Devise mitigation plans to reduce or redress harm in cases, where failure to comply with requests by the government may result in retaliation.
- (10) Cease lobbying activities and affiliations that may be at odds with company policies that respect rights.
- (11) Increase engagement on public policy in support of human rights and digital rights.
- (12) Design and implement corporate accountability measures and ensure meaningful input from stakeholders such as those utilizing these measures and the technical community.
- (13) Provide company level remedies and grievance redressal mechanisms both physical and virtual, to victims affected by adverse impacts of cybersecurity responses that violate their privacy.

6.4. Recommendations to Civil Society Organizations

- (1) Set up an independent multi-stakeholder body with the cooperation of various sectors to monitor the implementation of the Act, and to provide recommendations including with a view to adopting approaches that cause the least amount of harm to infrastructure and the individual.
- (2) Support the independent evaluation and analysis of substantive aspects, including the use of the principles of necessity and proportionality through established global standards, and the impact of responses on society and economy.
- (3) Contribute to the perspective on the Act, to balance the viewpoints of the largely military and defense centered perspectives shared, through the addition of a rights consideration, the interests of civil society and marginalized communities, the local context and the application of legislations therein.
- (4) Hold implementing authorities and officials liable for the misuse of their powers or information obtained, while carrying out their duties under the Act.

ENDNOTES

- 1 Bangkok Post, *Cyber threats ratcheting up*, (3 April 2018), available at: <https://www.bangkokpost.com/news/special-reports/1439667/cyber-threats-ratcheting-up>
- 2 Ministry of Digital Economy & Society, *Cybersecurity Act, B.E. 2562 (2019), Unofficial Translation*, available at: <http://www.mdes.go.th/assets/portals/1/files/Cybersecurity%20Act%20-%2028-06-2019%20-%20Clean.pdf>
- 3 As of 2017, Thailand Board of Investment, *Demographics*, available at: <https://www.boi.go.th/index.php?page=demographic>
- 4 United Nations Development Programme (UNDP), *Human Development Indices and Indicators: 2018 Statistical Update*, (2018), available at: http://hdr.undp.org/sites/default/files/2018_human_development_statistical_update.pdf
- 5 Hootsuite and We are social, *Digital 2019 Report*, (31 January 2019), available at: <https://datareportal.com/reports/digital-2019-global-digital-overview>
- 6 Freedom House, *Freedom in the World 2018*, available at: <https://freedomhouse.org/report/freedom-world/2018/thailand>
- 7 Reporters without borders, *2018 World Press Freedom Index*, available at: <https://rsf.org/en/ranking>
- 8 Freedom House, *Freedom on the Net 2018*, available at: <https://freedomhouse.org/report/freedom-net/2018/thailand>
- 9 Bangkok Post, *The cybersecurity balancing act*, (22 October 2018), available at: <https://www.bangkokpost.com/news/politics/1562230/the-cybersecurity-balancing-act>
- 10 International Telecommunications Union (ITU), *Global Cybersecurity Index 2017*, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- 11 Washington Post, *Thai military declares a coup, detains key political leaders*, (22 May 2014), available at: https://www.washingtonpost.com/world/asia_pacific/thai-military-declares-a-coup-detains-key-political-leaders/2014/05/22/5da6a6ca-e1a0-11e3-8dcc-d6b7fed081a_story.html?utm_term=.81b997dc2da3
- 12 Bangkok Post, *Senate dissolved, police chief sacked*, (24 May 2014), available at: <https://www.bangkokpost.com/most-recent/411568/prayuth-takes-total-control>
- 13 Freedom House, *Freedom on the Net 2018*, available at: <https://freedomhouse.org/report/freedom-net/2018/thailand>
- 14 Institute for Democracy and Electoral Assistance (IDEA), *Is the space for civil society really shrinking?*, (17 July 2018), available at: <https://www.idea.int/news-media/news/space-civil-society-really-shrinking>
- 15 Southeast Asian Press Alliance, *Thailand urged to lift free speech restrictions ahead of elections*, (18 December 2018), available at: <https://www.ifex.org/thailand/2018/12/17/thailand-lifts-free-speech-restrictions/>
- 16 The Nation, *Junta reins in Lese majeste*, (1 December 2018), available at: <http://www.nationmultimedia.com/detail/politics/30355507>
- 17 Dr. Janjira Sombatpoonsiri, *Manipulating Civic Space: Cyber Trolling in Thailand and the Philippines*, German Institute of Global and Area Studies (GIGA) Focus, (June 2018), available at: https://www.researchgate.net/publication/327931883_Manipulating_Civic_Space_Cyber_Trolling_in_Thailand_and_the_Philippines
- 18 Freedom House, *Freedom on the Net 2018*, available at: <https://freedomhouse.org/report/freedom-net/2018/thailand>
- 19 Dr. Janjira Sombatpoonsiri, *Manipulating Civic Space: Cyber Trolling in Thailand and the Philippines*, German Institute of Global and Area Studies (GIGA) Focus, (June 2018), available at: https://www.researchgate.net/publication/327931883_Manipulating_Civic_Space_Cyber_Trolling_in_Thailand_and_the_Philippines
- 20 The Nation, *Lifftin of political ban 'partial'*, (12 December 2018), available at: <http://www.nationmultimedia.com/detail/politics/30360215>
- 21 Nikkei Asian Revie, *Thai election turnout at 75% with pro-junta ahead in popular vote*, (28 March 2019), available at: <https://asia.nikkei.com/Politics/Thai-election/Thai-election-turnout-at-75-with-pro-junta-ahead-in-popular-vote>
- 22 Japan Times, *Will the Thai election be free and fair?*, (21 March 2019), available at: <https://www.japantimes.co.jp/opinion/2019/03/21/commentary/world-commentary/will-thai-elections-free-fair/#.XKqBzC2B28U>
- 23 Khaosod English, *Poll observers not confident election free or fair*, (24 March 2019), available at: <http://www.khaosodenglish.com/politics/2019/03/24/poll-observers-not-confident-election-free-or-fair/>
- 24 Krisdika, *Constitution of the Kingdom of Thailand B.E. 2560 (2017) Official Translation*, (2017), available at: [http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/Constitution_of_the_Kingdom_of_Thailand_\(B.E._2560_\(2017\)\).pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309](http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/Constitution_of_the_Kingdom_of_Thailand_(B.E._2560_(2017)).pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309)
- 25 DLA Piper, *Data protection laws of the world; Thailand*, (2017), available at: <https://www.dlapiperdataprotection.com/index.html?t=law&c=TH>
- 26 Krisdika, *Constitution of the Kingdom of Thailand B.E. 2560 (2017) Official Translation*, (2017), Sections 34 and 36, available at: [http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/Constitution_of_the_Kingdom_of_Thailand_\(B.E._2560_\(2017\)\).pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309](http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/Constitution_of_the_Kingdom_of_Thailand_(B.E._2560_(2017)).pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309)
- 27 Krisdika, *Constitution of the Kingdom of Thailand B.E. 2560 (2017) Official Translation*, (2017), Section 34, available at: [http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/Constitution_of_the_Kingdom_of_Thailand_\(B.E._2560_\(2017\)\).pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309](http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/Constitution_of_the_Kingdom_of_Thailand_(B.E._2560_(2017)).pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309)
- 28 Krisdika, *Constitution of the Kingdom of Thailand B.E. 2560 (2017) Official Translation*, (2017), Section 36, available at: [http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/Constitution_of_the_Kingdom_of_Thailand_\(B.E._2560_\(2017\)\).pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309](http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/Constitution_of_the_Kingdom_of_Thailand_(B.E._2560_(2017)).pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309)
- 29 International Labour Organization (ILO), *Thailand Penal Code Thai Criminal law*, available at: http://ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=82844
- 30 Thailand Law Library, *Torts (Section 420-437) Civil and Commercial Code*, (2015) available at: <http://library.siam-legal.com/thai-law/civil-and-commercial-code-torts-section-420-437/>
- 31 Krisdika, *Computer Crime Act 2007 (unofficial translation)*, available at:

<http://www.krisdika.go.th/wps/wcm/connect/70bf3700422d685491d69fd23e4afdc2/ACT+ON+COMMISSION+OF+OFFENCES+RELATING+TO+COMPUTER%2C+B.E.+2550+%282007%29.pdf?MOD=AJPERES&CACHEID=70bf3700422d685491d69fd23e4afdc2>

- 32 International Comparative Legal Guides (ICLG), *Telecoms, Media and Internet 2019: Thailand*, (21 November 2018), available at: <https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/thailand>
- 33 Krisdika, *Commission of Computer-Related Offences Act (No.2)*, B.E. 2560 (2017), (2017), available at: <http://www.krisdika.go.th/wps/wcm/connect/16aa6600426df0df92a9da09167c07d3/COMMISSION+OF+COMPUTER-RELATED+OFFENCES+ACT+%28NO.+2%29%2C+B.E.+2560+%282017%29.pdf?MOD=AJPERES&CACHEID=16aa6600426df0df92a9da09167c07d3>
- 34 Article 19, *Thailand Computer Crime Act*, (31 January 2017) p.2, available at: <https://www.article19.org/data/files/medialibrary/38615/Analysis-Thailand-Computer-Crime-Act-31-Jan-17.pdf>
- 35 LawPlus Ltd., *Amendments to Computer Crimes Act of Thailand Finally Published*, available at: <https://www.lawplusltd.com/2017/02/amendments-computer-crimes-act-thailand-finally-published/>
- 36 Haruethai Boonklomjit, Natpakal Rerknithi, Anna Gamvros, Ruby Kwok, *Overview of Thailand Draft Personal Data Protection Act*, (6 August 2018), available at: <https://www.dataprotectionreport.com/2018/08/overview-of-thailand-draft-personal-data-protection-act/>; Manushya Foundation, *(Draft) Personal Data Protection Act B.E. Unofficial Translation*, (2019)
- 37 DLA Piper, *Data protection laws of the world; Thailand*, (2017), available at: <https://www.dlapiperdataprotection.com/index.html?t=law&c=TH>; Thai Netizen Network, *Data Privacy in Thailand: Time to take off*, (27 July 2013), available at: <https://tinyurl.com/ya2hb9vj>
- 38 DLA Piper, *Data protection laws of the world; Thailand*, (2017), available at: <https://www.dlapiperdataprotection.com/index.html?t=law&c=TH>
- 39 E27, *Thailand now has six digital bills welcoming Thailand 4.0*, (13 February 2019), available at: <https://e27.co/thailand-now-has-six-digital-bills-welcoming-thailand-4-0-20190213/>
- 40 Ministry of Digital Economy & Society, *Cybersecurity Act*, B.E. 2562 (2019), *Unofficial Translation*, available at: <http://www.mdes.go.th/assets/portals/1/files/Cybersecurity%20Act%20-%2028-06-2019%20-%20Clean.pdf>; Manushya Foundation, *(Draft) Personal Data Protection Act B.E. Unofficial Translation*, (2019)
- 41 International Telecommunications Union (ITU), *Protection of Critical National Infrastructure*, (6-8 February 2012), available at: https://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B0000100043PPTe.ppt
- 42 As defined by International Organization for Standardisation (ISO) and International Electrotechnical Commission (IEC) 27000 in the following manner: Confidentiality is to ensure that information is only accessed by those authorized to do so; integrity is to ensure accessible and credible information, and availability is to ensure persons who are authorized can access information and associated assets when required. José Manuel Gaivéo, 'Security of ICTs Supporting Healthcare Activities' in *Handbook of Research on ICTs for Human-Centered Healthcare and Social Care Services*, IGI Global, (2013), pg. 210, available at: <https://bit.ly/2k2NkfN>
- 43 Necessity includes a legitimate aim and that which is least likely to infringe human rights. Electronic Frontier Foundation (EFF), *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*, available at: <https://necessaryandproportionate.org/principles>; and Electronic Frontier Foundation (EFF), *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*, (May 2014), available at: <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf>
- 44 Proportionality requires the high probability towards fulfilling a legitimate aim, with less invasive methods being exhausted or futile, with only relevant and material information related to a threat being accessed, with excess information that is collected being destroyed, and with access of information being carried out by those authorised for the purpose and duration that a threat exists. Electronic Frontier Foundation (EFF), *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*, available at: <https://necessaryandproportionate.org/principles>; and Electronic Frontier Foundation (EFF), *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*, (May 2014), available at: <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf>
- 45 As defined by International Organization for Standardisation (ISO) and International Electrotechnical Commission (IEC) 27000 in the following manner: Confidentiality is to ensure that information is only accessed by those authorized to do so; integrity is to ensure accessible and credible information, and availability is to ensure persons who are authorized can access information and associated assets when required. José Manuel Gaivéo, 'Security of ICTs Supporting Healthcare Activities' in *Handbook of Research on ICTs for Human-Centered Healthcare and Social Care Services*, IGI Global, (2013), pg. 210, available at: <https://bit.ly/2k2NkfN>
- 46 Prachatai, เสวนาสมาคมนักข่าวชี้ พ.ร.บ.ความมั่นคงไซเบอร์ เสี่ยงละเมิดสิทธิเสรีภาพประชาชน, 27 October 2018, available at: <https://prachatai.com/journal/2018/10/79320>
- 47 Prachatai, เสวนาสมาคมนักข่าวชี้ พ.ร.บ.ความมั่นคงไซเบอร์ เสี่ยงละเมิดสิทธิเสรีภาพประชาชน, 27 October 2018, available at: <https://prachatai.com/journal/2018/10/79320>
- 48 Bangkok Post, *Taking up the fight against 'fake news'*, 29 August 2019, available at: <https://www.bangkokpost.com/opinion/opinion/1738763/taking-up-the-fight-against-fake-news?fbclid=IwAR3Axxh9aPnDKMv8E9fyJW32S6XbgxssMiWRgB8uGiMFvv4RrhhYdLapx-z0>



MANUSHYA

Empowering Communities | Advancing Social Justice

About Manushya Foundation

Founded in 2017, Manushya Foundation serves as a bridge to engage, mobilise, and empower agents of change by: connecting humans through inclusive coalition building and; by developing strategies focused at placing local communities' voices in the centre of human rights advocacy and domestic implementation of international human rights obligations and standards.

Manushya Foundation strengthens the solidarity and capacity of communities and grassroots to ensure they can constructively raise their own concerns and provide solutions in order to improve their livelihoods and the human rights situation on the ground.

CONTACT US:

-  5/4 Thanon Suthisan Winitchai 1, Samsen Nai, Phayathai, Bangkok 10400, Thailand
-  contact@manushyafoundation.org
-  +66 (0) 945-811-827
-  www.manushyafoundation.org
-  facebook.com/ManushyaFdn
-  twitter.com/ManushyaFdn