28th March 2018

Ms. Ajarin Pattanapanchai
Permanent Secretary
Ministry of Digital Economy and Society
120 Moo 3, 6-9 floor The Government Complex
Commemorating His Majesty, Chaeng Watthana Road,
Thung Song Hong,Khet Laksi Bangkok 10210

By email to:
ajarin.p@mdes.go.th
sataporn.s@mdes.go.th
darunee.p@mdes.go.th

Ms. Ajarin Pattanapanchai

The Asia Internet Coalition (AIC) is an industry association made up of leading internet and technology companies. The AIC seeks to promote the understanding and resolution of Internet policy issues in the Asia Pacific region. Our Members include Google, Facebook, Apple, Twitter, LinkedIn, Expedia, Rakuten, LINE and Yahoo. We thank the Thai Government for seeking comments on The Cyber Security Act, and additionally for Khun Sataporn of your office agreeing to extend the deadline to 28th March in order for us to consolidate feedback from our members. We hope that consideration can be given to our points.

OVERVIEW

Cybersecurity is a serious global concern. In the World Economic Forum's Global Risk Report 2017, "large cyber attacks" came in sixth among the risks likely to happen in the next 10 years. We wish to congratulate the Royal Thai Government for its commitment to addressing cybersecurity issues. Privacy and cybersecurity are important to our members and their users. It is vital to find the right balance between protecting security and privacy, and one hand, and enabling businesses and innovation on the other.

We however have significant concerns about aspects of the Cyber Security Act in its current form. We appreciate being given an extension to submit comments, and understand the Government's need and desire to act quickly. However, we feel that we could have provided significantly more useful insights had we had more time to draft our comments, and appreciate that we would be given more lead time in future consultations. Nonetheless, we sincerely appreciate the extension and hope that our comments will be useful.

One key concern that we would have liked time to consider further, is that the Cyber Security Act potentially overlaps with the hacking provision under the Computer Crime Act. Global experience indicates it is not helpful to have overlapping laws, as it can lead to confusion and inconsistency. It would be useful to understand from the government's perspective how this would relate to the other digital economy laws.

Another area of concern is that numerous government entities would be authorised to use their own enforcement powers under this draft act. This may lead to inconsistent and uneven enforcement.

The Act seems to create a distinct Cybersecurity Office. We note that this can be a useful approach but it quickly poses problems if the new offices has authorities that overlap substantially with existing authorities of other law enforcement/investigative bodies. This seems especially likely here, where the office seems to have both proactive responsibilities (e.g., directing agencies to secure their systems) and reactive responsibilities (investigating breaches when they occur). We would be interested to know how the Royal Thai Government intends to deal with overlapping authorities when this inevitably arises.

Additionally, the new office is tasked with both proactive cybersecurity work and reactive investigative work. We submit, bearing in mind other international frameworks, that this combination is often unhelpful in a cybersecurity authority. Cybersecurity is more effective when it is distinct from law enforcement so that private sector organizations will trust and engage with them. We therefore recommend that the Government consider a change in approach here.

Definition of Cyber Security harms

We welcome the Thai Government's efforts to define relevant wording in the text, as set out in Article 3. However, we note that some key definitions are absent. The Act refers to harmful cyber activities, and harmful cyber events, without any clarity as to the definition or either or the difference between the two, if there is in fact any difference. "Harmful event" is references in Article 14 (d) and referenced in the definition of Cyber Security in Article 3. "Harmful Cyber event/s" is referenced in 7 (iii), 7 (vi) and 14 (iv). "Harmful Cyber Activities" is referred to in Article 5, and "Harmful Activities" in Article 15 (iv). The term "Cyber Harm" is also not defined, and referenced 35 times in the Act. We suggest that these terms be defined and used consistently for clarity. "Cyber Security harm/s" remains undefined. We feel that it would be highly beneficial to provide a detailed definition. We note no reference to "cyber attack" which would be the more commonly used terminology.

Lack of Court Order Requirements – Articles 34, 36, 37, 39, 41, 42, 43, 44, 45, 46, and 47

These Articles give the Minister of MDES, the Cyber Security Commission, other cyber security government authorities, the Office of the Cyber Security Commission, and the officers under the Draft Law the authority to command, request and order private organizations to act, not to act, request cooperation, request personnel and/or equipment, summons persons and documents, and/or request compliance with the Commission's order under certain circumstances without a court order. We would submit that even in urgent cases, it should be possible to obtain an expedited court order and would ask that consideration be given to making this a requirement throughout the Act, as we note further powers to act without a court order in Articles. We note the limited exceptions in Section 44, where the Office of the Cyber Security Commission must obtain a court order to use communication or electronic devices to track cyber harms which results in affecting rights of other persons; and Section 47 (3) whereby the officers under the Draft Law are authorized to access communication data upon a court order. However, in case of emergency, the officers can obtain an approval from the Commission and report to the court later. As previously stated, we submit that in all occasions it should be possible to obtain a court order on an expedited basis, and that this is beneficial for both transparency and due process.

Article 40

"In the case where any of the following events occur, it shall be assumed that there is or there will be a Cyber harm:

(i) a communication of information which is so abnormal that it is reasonable to speculate that such communication is a result of a Cyber harm;

(ii) an attempt to access or login to the information system or the communications system using an external technology, which is so abnormal that it is reasonable to speculate that such communication is a result of a Cyber harm;

(iii) the information system or the technology-based communication system is destroyed from which it can be reasonably inferred that a Cyber harm has occurred; or

(iv) any other event as the Commission shall prescribe."

As mentioned above, the lack of a definition for "Cyber harms" is particularly evident here and makes understanding and responding to this provision challenging. Firstly, (i) and (ii) are incredibly broad. Essentially, it seems that any communication or access attempt that is sufficiently "abnormal" can be considered a cyber harm. Further, the Commission has the authority to define "any other event" as a cyber harm under (iv). Essentially, the Commission is granted expansive powers when there is a cyber harm, and then given the authority to define when there is a cyber harm. We are concerned that this could discredit the Thai Government and cause its motives to be questioned as without a set definition, the Government could continually expand what is considered to be a Cyber harm. Additionally, we submit that (iii) is seems very narrow. It isn't clear to us when an information system is considered "destroyed." Would a reboot count? Do the physical technology components have to be so broken that they won't turn on? Again, further detail and definitions here would improve the clarity and consistency of the law. As it stands at present, the scope of what is or what

is not a cyber security harm relies mainly on the discretion and interpretation of the relevant government authorities.

Article 41

"In the event where there is or it is speculated that there is a Cyber crime in the information technology which is within the responsibility of any state agency related to the maintenance of Cyber Security, such state agency shall be step in to prevent, stop, break, and remedy such Cyber harm, and that state agency shall have the following duties:

(i) deal with the Cyber harm, and upon discovering an obstacle or problem in dealing with such Cyber harm, request the Office for help;

(ii) report the harm and how it deals with such harm to the Office as soon as practically possible. In the case where it is speculated that a Cyber harm will occur to the state agency, such state agency or the responsible person, pursuant to article 38, shall report to the Office such harm;

Upon receipt of such report, pursuant to paragraph 1 of this article, the Office shall immediately coordinate with the organizations so mentioned in paragraph 1 to prevent or remedy such harm as appropriate and shall report so to the Commission. The Commission may issue any instruction accordingly as appropriate."

The Act refers to IT "which is in the responsibility of any state agency." We would like to clarify if this means IT that the agency operates, or IT within an industry that the agency regulates? For the former, only actual government systems are in scope. For the latter, any system within any regulated industry is in scope. We ask because if there is "or is speculated that there is" a cyber crime on any in-scope systems, government agencies are to step in and "deal with the Cyber harm". If this applies to private-sector systems within regulated industries, this grants the regulator extremely far reaching authority to act on private sector systems based on an extremely broad standard. As the government moves toward regulations of the industry in Thailand, this could have direct implications for industry companies' systems within the country if the broad scope applies here. We would ask that clarification is provided and that we are given a further opportunity to make submissions on any amendments.

Article 53-56 – Criminal Liability

"53. Any person who violates, or does not act in accordance with the Minister's instructions pursuant to article 46 paragraph 2 shall be subject to imprisonment not exceeding an imprisonment term of [] months, or a fine not exceeding [] baht, or both.

54. Any person who violates, or does not act in accordance with the Officer's instructions pursuant to article 47 shall be subject to imprisonment not exceeding an imprisonment term of [] months, or a fine not exceeding [] baht, or both.

55. Any person who violates article 48 paragraph 1 shall be subject to imprisonment not exceeding an imprisonment term of [] months, or a fine not exceeding [] baht, or both.

56. Any violation of or action inconsistent with article 46 paragraph 2 and article 47, provided such violation or action is a result of an instruction or absence of instruction or action or inaction of an authorized representative of a juristic person, such representative shall be subject to imprisonment not exceeding an imprisonment term of [] months, or a fine not exceeding [] baht, or both."

Firstly, the although the Act makes it clear that criminal penalties can/will be imposed, no details are given as to the extent of these. Articles 53-56 appear to be absolute, with no suggestion of a defence should the person in question not knowingly have breached the law, or done all that they could practically do in the circumstances to assist. This adds to the uncertainty of the Acts implementation and fears that it could be arbitrarily applied. In any case, it is submitted that criminal liability should be imposed only on the most egregious of breaches.

Summary

We do hope that our comments give the Royal Thai Government an insight into the industry perspective, and we will be more than happy to provide further comments or answer any further questions the Government may have.

Yours sincerely

Jeff Paine

Managing Director, Asia Internet Coalition