5th September 2017

Respectfully to: Ministry of Public Security
Hanoi, Vietnam

Attention: Senior Lieutenant General To Lam
The Minister

Comments on amendments to the Draft Law on Cybersecurity

The Asia Internet Coalition thank the Government of Vietnam for an opportunity to comment on the amendments made to the Draft Law on Cybersecurity. We were pleased to see that some positive changes have been made – for example the removal of criminal liability. However, as pointed out in our previous comments, the Draft Law needs to ensure that there are comprehensive definitions. It appears that the amended Draft Law has replaced "Cyber products" with "digital device" but the latter is not defined. This is crucial to, among things:

- Cybersecurity verification to be conducted before digital devices are put into use in information systems critical to national security (Article 12(1))
- Certification of compliance with technical regulations on cybersecurity to be conducted on digital devices before they are used in information systems critical to national security (Article 18(2))
- Article 60, where the provincial people's committee is empowered to "manage the quality of digital devices.."

At the very least, this imposes unclear bureaucratic requirements that could even hamper cybersecurity protection. Further to our suggestion to limit the definition of Cyber products and services in the previous draft we suggested that "digital device" be defined to be "a device intended to detect, mitigate, or prevent cybersecurity threats."

Among the Prohibited Acts in Article 8 is posting, preparing and dissemination of content that is "embarrassing". This appears to be even broader than what Decree 72 prohibits. We wish to reiterate our comments below that we strongly submit that content issues should be kept entirely separate from that of Cybersecurity.

Previous Comments

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, PayPal, Rakuten, LINE and Yahoo. We thank the Vietnamese Government for seeking comments on the Draft Law on Cyber Security and hope that consideration can be given to our points.

OVERVIEW

That cybersecurity is a serious global concern is not disputed. 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. In its submission on the Cybersecurity Draft Law, the Ministry of Public Security ("MOPS") notes that Vietnam's information network systems have suffered thousands of cyberattacks, losing thousands of billion Vietnamese dong each year.

We wish to congratulate the Vietnamese government for addressing cybersecurity issues, and particularly including in their strategy resources and training, support for a cybersecurity industry and support for research. We also appreciate and congratulate the Vietnamese Government for their international approach to this issue evident by consulting internationally, for research and development and of course for tackling cybercrime;

Privacy and cybersecurity are very important to both our members and their users. It is vital to find the right balance between protecting security and privacy and enabling businesses and innovation. We want to ensure the latest technology can be adopted in Vietnam. However, we feel that it is essential to ensure that speech issues are not mixed up with cyber security. Whilst we understand they may be interconnected, we urge the government to separate out the issues, and deal separately with:

- cyber security,
- data protection;
- and online criminal

  activity, including

  civil liberties issues

We see benefit in the use of clear language: a large percentage of internet users, including mobile users, are not technical experts, but still need to understand the main issues. There is a need for the Vietnamese Government to explain cyber security in a way that can be easily understood by all.

We would draw your attention to the fact that some countries, like Singapore also actively encourage the joint government-public sector development and use of secure systems (https://www.ida.gov.sg/Programmes-Partnership/Store/National-Cyber-SecurityMasterplan-2018)

As the Law envisages, it is important that the Vietnamese government ensure high quality Vietnamese contributions to global standards in a competition, market based, open and transparent and peer-reviewed environment.

As explained above, we sincerely recognise the need for the legislation, however we are concerned that there may be a perception that cyber security legislation is being misused for censorship. We are concerned some may highlight the following to argue this:

- 'The policy is to build a stable and healthy cyberspace where behaviours are in line with the rules, righteous and civilized activities are encouraged, and any violating acts are severely sanctioned under legislation'. (Art 4)
- The impact of intermediary liability on our companies for a very wide ranging set of offenses.
- 'Any organisation or individual violating any provision of this Law shall, subject to the nature and severity of such violation, be disciplined, penalized for an administrative violation, or subjected to a criminal prosecution; where any damage is caused therefrom, shall compensate therefor in accordance with legislation.' (Art 8)
- the potential clash of jurisdictions and the impact on foreign investment and research in Vietnam of applying Vietnam-specific legislation and regulation, especially legislation that requires licensing from and monitoring by the Vietnamese Government;

The Cybersecurity Draft Law, as currently Drafted, excludes key elements, which as discussed below, which put to question whether it is sufficient to address cybersecurity risks, or whether it will lead to additional concerns that would ultimately weaken the information systems infrastructure and environment in Vietnam.

The key areas of concern for this Draft Law are:

1. The scope of the Draft Law is too broad.
2. The Draft Law imposes onerous measures and liabilities on internet service providers that would potentially impede the digital economy and the growth of internet services in Vietnam.
3. The Draft Law will increase the difficulty and cost of doing business in Vietnam.

4. Vague appraisal procedures in relation to products and services used in Critical Systems may be inconsistent with WTO commitments.

5. Breaches of the Law should not be subject to criminal prosecution

6. Lack of clarity including clear definitions

7. Restrictions on Civil Liberties and extent of prohibited acts

KEY AREAS OF CONCERN FOR THE DRAFT LAW

1. The scope of the Draft Law is too broad

In its submission on the Cybersecurity Draft Law, the MOPS notes that the Draft Law is necessary "to assure conformity with international practices," citing examples of cybersecurity Laws in different countries. In these countries, however, cybersecurity is generally limited to maintaining the security of network and information systems, as can be seen from the examples below:

❖ Japan's Basic Act on Cybersecurity defines cybersecurity as necessary measures that are needed to be taken to safely manage information ... and to guarantee the safety and reliability of information systems and information and telecommunications networks. http://www.japaneseLawtranslation.go.jp/Law/detail_main?re=02&vm=02&id=2760

❖ Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive") "lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market." http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

❖ Korea's National Anti-Cyberterrorism Act defines Cyber Security as measures and responses through administrative, physical, technological means in order to protect information telecommunication infrastructure and information from cyber terrorism, and includes cyber crisis management. https://cybercrimetech.com/2013/04/south-koreannational-cyber-terrorism_13.html

❖ The Cybersecurity Act of 2015 of the United States defines "cybersecurity purpose" as the purpose of protecting an information system or information that is stored on, processed

by, or transiting an information system from a cybersecurity threat or security vulnerability. http://uscode.house.gov/view.xhtml?req=(title:6%20section:1501%20edition:prelim)

Based on the foregoing, the Draft Law fails to meet its objective to "assure a certain conformity of our country's cybersecurity tasks with international practices and assure the conditions for international integration in cybersecurity". Indeed, the inclusion of content regulation clauses (which as discussed below, are largely covered by existing regulations) threatens to draw away much needed attention from the need to address cybersecurity in its traditional formulation.

2. The Draft Law imposes onerous measures and liabilities on internet service providers that would potentially impede the digital economy and the growth of internet services in Vietnam

Current regulations, primarily Decree No. 72/2013/ND-CP, sets out what are deemed to be prohibited acts in relation to the provision and use of internet services. The list of prohibited acts under this decree already suffers from overbreadth and vagueness, and has been the subject of (see http://www.asiainternetcoalition.org/aic-comments-on-vietnams-Draftinternet-decree-on-internet-services-and-online-information/). This Draft Law does little to address the uncertainties brought about by Decree No. 72, and instead, in Articles 7 and 10(2), contains even broader and vaguer provisions as to what constitutes prohibited content.

This uncertainty and the potential liabilities imposed on internet service providers would tend to dampen innovation in the provision of internet services and, on a wider scale, the growth of the digital economy in Vietnam.

We have serious concerns with regard to Article 51 (3) (4) and (5), which reads:

3. Websites, web portals or specialized pages on social networks of agencies, organisations and individuals shall post information in accordance with legislation, and shall not provide, post or transmit information with any content inappropriate to the interests of the country.

4. Telecommunication and internet service enterprises and enterprises possessing information systems shall set up their mechanisms to authenticate information when users register digital accounts to assure the confidentiality and the honesty of registration

information. The registrants of such digital accounts shall be responsible to protect and use the accounts they create in accordance with legislation.

5. Foreign enterprises, when providing telecommunication and/or internet services in Vietnam, shall comply with Vietnamese legislation, respect the national sovereignty, interests and security of Vietnam and the interests of users, obtain licences for their operations, locate their representative offices and servers in which Vietnamese users data are administered in the territory of the Socialist Republic of Vietnam, secure user information and users' account information, and sanction violations stringently under legislation."

Article 51.3 should recognize that websites, web portals or social networks host content that are posted by their users, and thus would not be able to control what the users post. Similar to comments in relation to Article 34, there should be a clear legal process for addressing this issue that, consistent with international practices, should include judicial oversight in respect of requests for content removal.

Article 51.4 and 51.5 both set out requirements that do not reflect current realities, and are likely to stifle growth and innovation in the digital sector. Internet service providers are being required to authenticate information provided by their users. Foreign enterprises are required to obtain licenses, and locate officers and servers within Vietnam. These requirements may result in Vietnamese people being deprived of digital services, or having to pay more for these services, as these burdens become too onerous or costly.

Article 51.3 should recognize that websites, web portals or social networks host content that are posted by their users, and thus would not be able to control what the users post. Similar to comments in relation to Article 34, there should be a clear legal process for addressing this issue that, consistent with international practices, should include judicial oversight in respect of requests for content removal.

A similar effect is expected of the onerous obligation imposed on enterprises (information system owners, Telco's and ISPs) to put in place technical measures not just to delete but to prevent any anti-state online information (Article 10.5), as well as the following requirements:

- Articles 39.5 and 59.2 require enterprises to obtain business licenses, establish representative offices, and locate all servers "in which Vietnamese users data are administered" within Vietnam's borders.

- Article 55(1)(a) requires telecommunications and internet service providers to refuse to provide services to users who do not provide real personal information. Implicit in this requirement is the obligation to ensure the authenticity of a user's identity.

The Draft Law would require the government to promulgate regulations that would establish its right to "administer and control international internet connections," and declares that cybersecurity in "cross border telecommunication, internet and information services shall be governed by the State." As set out in Article 43. There are extensive reasons why the free flow of data helps the country's economy (and conversely, how localization requirements will discourage business development). The Data Localisation Requirements in the Draft Law will cause significant impact on SMB's as well as larger companies. The AIC website has three reports which outline the damage that data localisation policies can do and the benefits of free flowing data.

We respectfully highlight that it is not only foreign companies who will be affected by data localisation policies, in fact smaller companies are more likely to be Vietnamese and the cost for smaller businesses will be proportionately higher than for larger companies. As set out in the ECIPE report, the effect of Data Localisation is not simply that it will affect businesses, it will also affect GDP. According to the World Economic Forum, "the flow of digital information between countries, companies and citizens is increasingly recognized as a critical driver of economic growth and innovation, particularly in the age of the knowledge economy." At a time when Vietnam is looking to conduct an IT Law Review to benefit from the digital economy and promote Vietnam 4.0, data localisation policies should be avoided for the private sector. Companies should be allowed to choose the best option for their company regardless of location. Locating data servers locally does not increase cybersecurity for data and it can be counterintuitive as cybercriminals can more easily identify the location of the data for cyberattacks since the search zone is now narrowed down to data servers within a country (as opposed to letting companies decide globally where to locate their or their customers' data). An effective cybersecurity strategy is one where there is good execution of ever-evolving best practices in security to the combined areas of technology, processes, people and physical facilities.

Companies have made huge investments to ensure that their data centers are secure. Forcing companies to locate servers locally would make them more vulnerable to attack as the systems and network might be less sophisticated, and generally harder to update with the latest security software. We strongly suggest any data localisation requirement be limited to only Government information systems.

3. The Draft Law will increase the difficulty and cost of doing business in Vietnam

The requirements set out in the Draft Law threaten to increase the costs of doing business in Vietnam, for both foreign and local enterprises. Small & medium businesses (SMBs) in particular will be more negatively impacted as they have lesser resources to deal with the potentially rigorous licensing, audit and compliance requirements, including the following:

❖ Enterprises need to comply with MPS-directed national cybersecurity standards and audit requirements set out in Articles 19 to 22. This covers a wide range of industries, including chemical, commerce, information, energy, finance, agriculture & food, medical and healthcare, IT, materials, transport etc. as enumerated in Article 18.2d. It is suggested that the Law imposes obligations that are commensurate to the nature of the industry, lest these requirements have an inadvertent effect of creating disincentives to digitizing certain businesses.

❖ A license from the MPS is required for the business of providing cybersecurity assurance services. Article 32.2 of the Draft Law further states that this Law will prevail in cases of overlap with the Law on Cyber Information Security ("LOCIS"). Companies already licensed by the Ministry of Information and Communications ("MIC") under the LOCIS may run the risk of being subject to an additional license requirement by the MOPS when this Draft Law comes into effect. It is also unclear whether the license granted by the MOPS under this Law will exempt the licensing requirements under the LOCIS with regard to the same types of services.

Under Article 34.2(c) of the Draft Law, the applicant for a license must submit its business registration certificate or investment certificate. This seems to indicate that an entity incorporated outside Vietnam cannot obtain such a license and limiting competition.

4. Vague appraisal procedures in relation to products and services used in Critical Systems may be inconsistent with WTO commitments

Article 20.2(b) of the Draft Law requires that products and services intended to be used in Critical Systems be reviewed/appraised by the competent agency under the MOPS or by a professional organization authorized by the MOPS. However, the Draft Law contains no detail on any review / appraisal procedures, as well as on any objective criteria to establish whether a specific product or service is fit for use in Critical Systems. Vague review / appraisal procedures may result in non-transparent procurement procedures and discrimination between offshore suppliers and domestic suppliers. Additionally, the application of vague

appraisal procedures may constitute unnecessary technical barriers to trade or domestic regulations which are inconsistent with Vietnam's WTO commitments.

5. Breaches of the Law should not be subject to criminal prosecution

Article 8 of the Draft Law provides that violations of the Law may be subject to criminal prosecution, but does not specify which breaches would be deemed criminal. As noted above, the Draft Law deals with an overly broad subject matter well beyond what is traditionally in the sphere of cybersecurity. The broadness of the Draft Law, the vagueness of certain of its provisions and the absence of guidance as to which provisions attract criminal liability add to the uncertainty of the Law's implementation and fears that it would be arbitrarily applied.

In any case, it is submitted that criminal liability should be imposed only on the most egregious of breaches. There are, for example, administrative requirements for which the imposition of criminal penalties to address breach would be too harsh.

6. Lack of Clarity including clear definitions

The Draft Law does not use standard definitions of cyber security, and instead conflates cybersecurity with data protection and criminal use of the internet, for example, for terrorism or speech against the state. There is a consistent lack of clarity throughout the Law. It appears that the Law covers everyone using the internet and any organisation, but definitions lack clarity. For example, we are unclear as to the meaning of 'information systems of the information industry and sector'? (Art 18)

ISPs have to put in place technical measures to prevent the display of information that violates the wide-ranging definition 'any information on cyberspace against the State of the Socialist Republic of Vietnam, prejudicial to the legitimate rights and interests of any organisations or individuals, or contrary to the morality or the fine customs and practices.'

We also note that the term telecommunications provider" is undefined and would welcome a definition similar to "telecommunications carriers" in the US (that is, only internet service providers). For further comments on this please refer to point 7 below.

The Draft Law would require information system owners to coordinate with government cybersecurity agencies to identify the origin of cyberattacks perpetrated on the owners'

systems as set out in Article 12 & 4. Additionally, if the government declares that there is an increased risk of an "urgent circumstance as to cybersecurity," the Ministry of Public Security (MOPS) may require organizations to "collect and report related information in a timely fashion" and to coordinate with the agency to prevent an attack. Art. 16 §§ 1(a), 3. We recommend the Vietnamese Government limit the application of this provision to circumstances in which a cyberattack creates a risk of harm for users. We further suggest that it would be helpful for the term "related information" to be defined, in order that there is transparency and no accusations can be made that the Government is using this provision to extract unrelated information.

The Draft Law would deem certain information systems to be "critical to the national security," including those that are used in State-sponsored industries, those "affecting the national sovereignty, interests, and security," and those "seriously affecting the social order and safety," among others (referred to herein as "Critical Systems") as set out in Article 18 & 1. MOPS would have the authority to establish cybersecurity standards for Critical Systems and to audit them, including by analysing data derived from the systems and related documents, and to implement "technical solutions and professional operations" for any perceived deficiencies, as set out in Articles 20-21. Critical Systems operators would also be responsible for reporting any cybersecurity incidents and working with MOPS to remedy them, and MOPS would have the power to halt the Systems' operations during remediation, as set out in Article 22. We propose that Critical Systems be re-defined to include only systems that are part of the state-sponsored national infrastructure.

The Draft Law would require organizations to remedy "any security error or flaw" found in a "cyber product or service," and to notify users and authorities of any such flaws, as set out in Article 31 & 1(d). "Cyber products and services" are defined broadly to include "hardware, equipment and software, catering for the operations of cyberspace, or stored or transmitted thereon." We request that the Vietnamese Government limit this definition to security errors or flaws that are known to have compromised user security and that voluntary reporting is the most appropriate way to ensure appropriate transparency. We also seek to clarify that there is no requirement to reveal the exact nature of the flaw, as publicizing every security flaw could tip off criminals to new attack vectors.

The Draft Law leaves many questions unanswered, including:

- What is the legal process under the Law for addressing Law enforcement issues and government requests (i.e. will court orders, subpoenas be used to require company assistance and/ or to allow Law enforcement to investigate crimes under this Law)?
- What penalties are there for non-compliance?

- How will the Law handle conflict of Law issues?
- How does the Law recognise existing internal standards and best practice?

7. Restrictions on Civil Liberties and extent of prohibited acts

The Draft Law includes a very broad range of prohibited acts, including:

- The use of cyberspace to prejudice the national sovereignty, interests and security, or the social order and safety.
- Posts on cyberspace against the State of the Socialist Republic of Vietnam, prejudicial to the legitimate rights and interests of organisations or individuals, or contrary to the morality or the fine customs and practices.
- Unauthorized intrusions on or appropriations of information or documents.
- Cyberattacks.
- Cyberterrorism.

In addition to our concerns raised about the broadness and vagueness of this definition and its impact upon the digital economy in Vietnam as set out in Point 2 above, it seems that Article 8 holds 'any organisation violating the Law' responsible whilst Articles 9 and 10 allow the Vietnamese Government to 'temporarily suspend, suspend, or withdraw the operating licence of, the website or the web portal posting the information' of any individual calling on:

- 'people to join a mass gathering that disturbs the security and order';
- posting information that is:
- distorting a historical truth, negating a revolution achievement, or sabotaging the great national unity;
- distorting or defaming the people's government;
- being any fabrication or causing any confusion among the people;
- causing a psychological warfare, inciting an aggressive war, or causing enmities between nations and the people of countries;
- propagating reactionary thoughts;
- offending the nation, a famous person or national hero;
- fabricating, spreading or dispersing what are clearly known to be false to offend human dignity or honour, or to embarrass or slander any organisation or individual;
- instructing or inciting any acts in violation of legislation;
- prejudicial to the legitimate rights and interests of any organisation or individual, or contrary to the morality or the fine customs and practices on cyberspace.

The inclusion of this list of prohibited acts confuses and dilutes the stated objective of cybersecurity. The use of cybersecurity legislation for censorship and reporting of those censored, the Law appears to allows cybersecurity legislation to be used as a reason for blocking and filtering of content. Globally, cybersecurity does not include this type of activity.

The Draft Law advocates 'cyber security supervision' (Section 3) and 'licensing' (Section 4) which could be argued is akin to industrial espionage, and may require companies to register and receive certification to provide cyber security advice to users. Such a requirement will reduce the security of Any globally legitimate cybersecurity Law should have no role in this type of activity.

The Draft Law would prohibit “the use of cyberspace” to engage in certain types of speech, including speech that “prejudices the national sovereignty, interests and security, or the social or and safety,” and “posts on cyberspace” that are against Vietnam’s government or “contrary to the morality or the fine customs and practices” (referred to herein as “Prohibited Speech”) and as set out in Article 7 & 1-2. The Draft provides examples of Prohibited Speech, including “distorting or defaming the people’s government,” “causing confusion among the people,” and “offending the nation, a famous person or national hero,” among other categories, as set out in Article 10 & 2. It further states that organizations and individuals may not “produce, post, store, or disperse” the Prohibited Speech Articles 10 & 4.

We respectfully suggest you consider limiting the definition of “cyberspace” to only public internet channels on the grounds that it is not feasible for companies to monitor the content of messaging sessions, etc., even if a company had the technical capability to do so. We further seek to more narrowly define the categories of prohibited speech to include only concrete threats, such as terrorism, threats of violence, etc. This will assist in the perception of this Law as a genuine Law for security and not for control of content.

Further, with regard to mandatory cooperation with authorities to combat “mass gatherings disturbing the security and order” the Draft Law requires “telecommunications providers” (a term not defined in the Law) to “closely coordinate with the competent authorities in handling the information on cyberspace that incites mass gatherings disturbing the security and order.” As set out in Articles 9 & 3. We again propose that you consider limiting the definition of “telecommunications provider” to a definition similar to “telecommunications carriers” in the US (that is, only internet service providers).

The Draft Law would require telecommunication service providers to put in place “technical measures to prevent the displaying of, and delete,” the Prohibited Speech, as set out in Article 10 & 5. We recommend that Vietnam limit the filtering requirement only to publicly-available communications, on the basis that private communications between just one or a handful of people are unlikely to incite the undesired behaviour.

We once again congratulate the Vietnamese Government for its efforts in legislating this complex but vital area of Law. We do hope that our comments give the Vietnamese Government an insight into the industry perspective, and we will be more than happy to provide further comments or answer any further questions the Vietnamese Government may have.

Yours sincerely

Jeff Paine, Managing Director

Asia Internet Coalition