KEY SPEECH NOTE BY THE PROSECUTOR GENERAL OF THE SOCIALIST REPUBLIC OF VIET NAM AT THE 2018 CHINA – ASEAN PROSECUTORS GENERAL CONFERENCE

(Bandar Seri Begawan, Brunei, 13-15/8/2018)

Theme: Enhancing Capacities and Cooperation in Combating Cybercrime

---

H.E. Mr/Mrs Chairperson,

Ladies and Gentlemen!

On behalf of the delegation of the Supreme People's Procuracy of the Socialist Republic of Viet Nam, I would like to convey my warmest greetings to all participants at the 2018 China - ASEAN Prosecutors – General Conference, held in the hospitable and beautiful Kingdom of Brunei. First of all, allow us to express our sincere thanks to the Attorney General's Chambers of Brunei for your invitation and warm hospitality extended to the delegation of the Supreme People's Procuracy of Viet Nam during the Conference. We always appreciate this frequent cooperation mechanism between the Supreme People's Procuratorate of China and the Prosecutors Offices of ASEAN countries. During more than a decade, this Conference has been an important international forum in the region about legal issues. Topics of the last Conferences have provided us with precious knowledge and experience in law making as well as practices of law enforcement in penal and criminal procedural laws in Viet Nam.

Ladies and Gentlemen!

Cybercrime is type of high-technology criminals that often utilize well-advanced knowledge, skills, divices, instruments to illegaly affect information, data, signals stored, processed, transmitted in computer systems, tele-communication networks or digital devices, which violate information security and order, damage governmental benefits and legal rights and benefits of individual and entities.

In recent years, Viet Nam as well as other countries in the world have been challenged and suffered from massive cyber attacks in general as well as cybercrimes in particular. Hackers intrude into data systems of public offices, entities and individuas at large scale in order to commit criminal activities such as asset and data appropriation, malwares installation, transnational gambling, blackmail, prostitution broker, narcotic and counterfeit trading, fake news and pornography dissemination etc. In 2017, computer viruses made Vietnamese Internet users loss 12.3 billion VND (equivalent to 540million USD)[1]. More seriously, there have been numerous propaganda activities on cyberspace to aggressively protest the Government, provoke violent demostration and support extreme conduct for the purpose of making the society chaotic. Facing such unforeseen development of this crime, the twenty-seventh session of the Commission on Crime Prevention and Criminal Justice under the United Nations was underway in Vienna, Austria from 14-15 May, 2018 to work on measures of cooperation to fight agaisnt cybercrime and this topic is planned to be discussed at the Fourteenth United Nations on Crime Prevention and Criminal Justice held in Tokyo in 2020. For us, we are determined that it is critical and necessary to improve relevant legislations on cybersecurity and enhance international coopeartion on this issue.

Ladies and Gentlemen!

In recognition of the importance to enhance the effectiveness of the fight against crime at any kind as well as cybercrime, Viet Nam has focused on making and finalizing penal and criminal procedural legislations in connection to this criminal conduct.

The Vietnamese Penal Code 2015, amended and supplemented in 2017 introduced new provisions on cybercrime-related offences as follows:

Firstly, the new Penal Code sets out a separate sub-chapter, providing for 09 information technology and telecommunication-related offences2, including 04 newly criminalized ones, specifically as follows:

[1] People's News Paper No. 22897 19 June 2018.

[2] Sub-Chapter 2 of Chapter 21 of the Vietnamese Penal Code 2015, amended and supplemented in 2017: High-Technology and Telecommunication Offences:

Article 285. Offence of illegally producing, trading in, exchanging, publishing offering equipment, devices, softwares to utilize for illegal purposes;

01. Offence of illegally producing, trading, exchanging, publishing and offering equipment, devices, softwares to utilize for illegal purposes (Article 285);

02. Offence of illegally collecting, possessing, trading in, exchanging or publishing information of bank accounts (Article 291);

03. Offence of illegally utilizing radio frequency which is solely utilized for purpose of medical emergency, safety, search and rescue, national defence and security (Article 293);

04. Offence of intentionally causing harmful interference (Article 294).

Secondly, the new Penal Code abolished ambiguous elements to constitute some cybercrime-related offences, such as "causing serious consequences, very serious consequences or extremely serious consequences" and is replaced with concrete elements of consequences of all these offences. For example, elements of illegal proceeds of crime or damages are specified with certain amounts of money; or elements of affected digital devices or information systems are specified with certain number of people as victims; or element of privacy affected is added with the victim's suicide as consequence etc.

Thirdly, pecuniary penalties as main punishments are widely applied to information technology and telecommunication-related offences categorized as less serious or serious crimes, ranging from 20 million VND to 1.5 billion VND.

Article 286. Offence of dispersing computer programs causing damages to the operation of computer networks or telecommunication networks;

Article 287. Offence of obstacling or disordering the operation of computer networks or telecommunication networks;

Article 288. Offence of illegally supplying or utilizing information of computer networks or telecommunication networks;

Article 289. Offence of illegally intruding into computer networks, telecommunication networks or digital devices of other persons;

Article 290. Offence of utilizing computer networks, telecommunication networks or digital devices to obtain assets;

Article 291. Offence of illegally collecting, possessing, trading in, exchanging or publishing information of bank accounts;

Article 293. Offence of illegally utilizing radio frequency which is sololy utilize for purpose of medical emergency, safety, search and rescue, national defence and security;

Article 294. Offence of intentionally causing harmful interference.

In addition, in the new Penal Code, the amount of pecuniary penalties as additional punishments is increased for eight out of nine offences mentioned above.

Apart from new changes in the 2015 Vietnamese Penal Code, the 2015 Vietnamese Criminal Procedural Code has officially recognized electronic data is a source of evidence, and is supplemented with new provisions specifying steps to seize and store digital evidence.

These above amendments both facilitate the fight against cybercrime more fully and thoroughly in the manner of prosecuting right offenders for right offences and help effectively prevent and intercept this kind of criminal conduct as well as its economic consequences.

Ladies and Gentlemen!

Despite of initial achievement, the fight agaisnt cybercrime still faces challenges and diffilcuties. Specifically as follows: (1) the nature of cyberspace is borderless and undetectable that causes difficulties in discovering criminal conduct and obtaining evidence; (2) legal system differences among countries in the way to collect digital evidence can worsen the effectiveness of mutual legal assistance to seek for digital evidence from foreign countries; (3) human resources and infrastructures in Viet Nam allocated to the fight against cybercrime have been limitted and (4) specilized law enforcement officers' capacity still lacks relevant intensive knowlege and experience to deal with IT crime.

Therefore, for the effectiveness of the prevention and suspression of kind of crime, we respectfully suggest the followings:

Firstly, there is a need to make a comprehensive, syncronized and internationalized legal framework in order to deal with complicated development of cybercrime. As Viet Nam is in progress to finalize its legal system in general as well as legislation on anti-cybercrime in partucular, we are willing to learn from other countries of experience of this issue.

Secondly, it is necessary to enhance international cooperation to establish networks and build trust among central authorities for mutual legal assistance to effectively and timely collect digital evidence at both regional and international scale.

Thirdly, we should frequently organize conferences, serminars and training courses at various levels to help enhance capacity of investigation, prosecution and adjudication of cybercrime cases, and organize law enforcement officer exchange programs to enhance mutual understanding and expertise in combating high-technology crime.

Ladies and Gentlemen!

In order to cope with current status as well as future threats of cyber attacks, in June 2018, the Vietnamese National Assembly passed the Law on Cybersecurity. This law contains 06 Chapters and 43 Articles, governing activities of national security, public order and safety protection on cyberspace, responsibility of relevant authorities, entities and individuals. The law also demonstrates Viet Nam's efforts to deal with cybercrime; notwistanding, we kindly seek for cooperation and interests from regional and international colleagues during performing our functions and tasks in the prevention and suppression of this plague.

Finally, I would like to offer my sincere thanks to the Attorney General Chambers of Brunei for your kind invitation and warm hospitality and giving us opportunity to deliver these remarks in this event. I wish our Conference a great success and thank you very much for your attention!