ZURAINI HAJI SHARBAWI

SOLICITOR GENERAL

ATTORNEY GENERAL'S CHAMBERS,

BRUNEI DARUSSALAM

THE 11TH CHINA-ASEAN PROSECUTORS-GENERAL CONFERENCE

BANDAR SERI BEGAWAN, BRUNEI DARUSSALAM

YANG BERHORMAT, DATO PADUKA HAJI HAIROL ARNI BIN HAJI ABDUL MAJID,
ATTORNEY GENERAL, BRUNEI DARUSSALAM

HIS EXCELLENCY MR. ZHANG JUN
PROSECUTOR GENERAL, SUPREME PROCURATORATE, THE PEOPLE'S REPUBLIC OF CHINA

ATTORNEYS AND PROSECUTORS GENERAL

ESTEEMED SENIOR OFFICIALS, DISTINGUISHED GUESTS

LADIES AND GENTLEMEN

"ENHANCING CAPABILITIES AND COOPERATION IN ADDRESSING CYBERCRIME"

Let me begin by echoing Yang Berhormat Dato's earlier sentiments, and personally welcome all delegates to Brunei Darussalam. We hope that you will enjoy your stay and that your experience here in Brunei Darussalam and specifically during this conference will be both productive and enjoyable.

INTRODUCTION

Excellencies, Distinguished Delegates, Ladies and Gentlemen

The chosen theme for this year's 11th China-ASEAN Prosecutors-General Conference is *"Enhancing Capabilities and Cooperation in Addressing Cybercrime".* As you can clearly see, a more focused approach has been taken with the substantive theme for this year's conference compared to previous years. While the themes of previous years' conferences have been more general in nature, this year's theme recognises cybercrime as a growing challenge, not just within the ASEAN region, but globally as well,

and the importance of trying to deal with the rapid advancement of cybercrime.

This is further emphasised at the regional level by the establishment of the ASEAN Cyber Capacity Program (ACCP) and the ASEAN Cybersecurity Cooperation Strategy and the identification of Cybercrime as one of the ten priority areas under the ASEAN Ministerial Meeting on Transnational Crime and the ASEAN Senior Officials Meeting on Transnational Crime (AMMTC/SOMTC) which underscore ASEAN's unwavering commitment, as well as at the global level, with the prominent theme and thematic debate at the recent 27th Session of the United Nations Commission on Crime Prevention and Criminal Justice focusing on criminal justice responses to preventing and countering cybercrime in all its forms.

It is clear that some of the main reasons for the rapid growth of cybercrime and its associated challenges is due to globalization, the mass use of the internet, and widespread and unprohibited use of social media. Together with this growth comes the increasingly uphill task for law enforcement agencies and prosecutors alike to hold perpetrators accountable for cybercrime offences committed via such platforms.

It therefore becomes incumbent on governments to come up with possible responses to these challenges, and formulate appropriate and innovative ways to combat cybercrime and to ensure that perpetrators do not get away with circumventing the laws and regulations we have in place.

THE BRUNEI DARUSSALAM EXPERIENCE

Excellencies, Distinguished Delegates, Ladies and Gentlemen,

Brunei Darussalam has a legal framework to address cybercrime offences as well as cyber-enabled crime through the use of various laws.

Our Computer Misuse Act, Chapter 194 deals with offences where the Computer is the target as well as where Computers are used to facilitate offences. Examples of these are unauthorised access of computers, unauthorised modification of computer material as well as obstruction of computer use.

We also utilise the Penal Code, Chapter 22 which contains the relevant provisions to legislate against certain forms of activities that may occur in cyberspace or forms of cyber-enabled crime where computers are the medium to commit further offences. Examples: offence of sexual grooming, possession of child pornography, criminal intimidation as well as criminal defamation. Online Fraud, for example can be prosecuted through the traditional offence of Cheating.

Brunei Darussalam has established several implementing mechanisms in order to ensure that the cyber threat landscape in relation to Brunei Darussalam is constantly monitored. In 2016, the Cybersecurity Working Group was established under the National Security Committee under the Prime Minister's Office aimed at operating at a strategic level to coordinate information sharing amongst stakeholders and formulate joint action plans to address cybercrime and cybersecurity matters. In 2017, the Brunei Darussalam National Cybersecurity Framework was completed, with the objective of coordinating all cybersecurity related efforts and risk mitigation from multiple cyber-related agencies. The framework defines minimum and mandatory security requirements on issues such as risk management and compliance. It also provides guidelines on Critical Information Infrastructure Protection

(CIIP) as well as a standard approach to share critical information on Cyber Incidents accurately and in a timely manner. I am confident that such measures will result in better institutional coordination to ensure that Brunei Darussalam's cyber defenses are cohesive and robust.

Brunei Darussalam also places the utmost emphasis and priority where the protection of children and the younger generation is concerned. I am pleased to announce that in 2013, Brunei Darussalam became the first country in our region to establish a Child Online Protection Framework built upon the International Telecommunications Union (ITU) – Child Online Protection Initiative. Such a framework is necessary in coordinating the actions of stakeholder agencies in ensuring that the necessary measures are in place to ensure child safety online during a time when children and young persons increasingly use social media to communicate and become vulnerable to cyber bullying, harassment and sexual predators. I am also pleased to observe that increasing measures have been made by the local authorities to address the vulnerabilities in our system based on the framework assessment to ensure greater protection of our younger generation. The Content Advisory Council, a national body comprising members from various Government agencies, including

the Attorney General's Chambers, also plays a role in protecting users from online threats through the monitoring of online content that goes against the cultural, social and religious norms of Brunei Darussalam, by ensuring compliance with broadcasting codes and ethics to preserve national harmony.

I am pleased to report that the Attorney General's Chambers has also set up a Cybercrime Focus Group whose main aim is to ensure that Brunei Darussalam's legal measures against Cybercrime are in line with international standards such as the Budapest Convention as well as to coordinate effective prosecutorial strategy and develop cybercrime related expertise in addressing cybercrime threats. The Group is currently amending the Computer Misuse Act, Evidence Act, Criminal Procedure Code as well as the Penal Code to include more offences relating to cybercrime in order to keep up with the pace of technology as well as to address the issue of social media offending. The amendments also include proposals to enhance the powers of law enforcement agencies in investigating offences of a technological nature and easing procedures with this regard.

The Attorney General's Chambers has also been actively raising awareness amongst schools and the public on the dangers

of cybercrime, with focus being on the use of social media as a platform for such offences. Since the start of the campaign in 2013, the Chambers has, either solely or jointly with other agencies, organized a total of 70 cybercrime awareness talks.

Even with all these efforts, with the threat that cybercrime poses to both governments and private individuals alike, this is not enough.

Brunei Darussalam has also experienced several small scale cyber security threats in recent years, including intrusions such as denial of service attacks, non-compliance activity, malicious logic and various level intrusions that affected government websites and services. The use of the internet and social media to further extremism and terrorism propaganda has also found its way to Brunei Darussalam, and there have been several cases where legal action was taken against individuals that were involved in extremism and terrorism related activities. For example, in 2018, the Internal Security Department detained a 42 year old local man with links to Islamic State (IS) who had been found to have been using the internet and social media platforms, to further extremist views and to promote self-radicalisation among locals to support the IS cause overseas. He was also found to have been promoting

Brunei Darussalam through the internet and social media to attract militants and supporters outside the country. Another similar case involved a 34 year old local woman who had also become self-radicalised through social media.

CHALLENGES IN COMBATING CYBERCRIME

Excellencies, Distinguished Delegates, Ladies and Gentlemen.

There are many challenges that we need to overcome if we want to continue the fight against cybercrime, but we must persevere.

One of the main challenges is the fact that such crimes often transcend global and regional boundaries. This indeed poses a challenge to the effective and efficient investigations of such crimes, what more the prosecution thereof. It is often emphasized in both global and regional fora that international cooperation needs to be enhanced to facilitate the investigations and prosecution of such transnational crimes. However, it must be acknowledged that most jurisdictions already have in place

international cooperation legal frameworks and mechanisms to serve this purpose.

Thus it begs the question, why are the criminals still able to circumvent these laws and avoid being brought to justice? The inevitable answer is this – our international cooperation mechanisms need to be more innovative, matching the technology with which the criminals are committing the cybercrimes, centered on the development of quick and efficient responses to facilitate investigations and prosecutions of such crimes within the legal process.

PROPOSED RESPONSE

i. The need for legal provisions on data preservation to combat cybercrime

As we are all well aware, the attractiveness of cybercrime lies in its swift and anonymous nature where with a click of a few buttons, the criminal can commit the crime and extricate himself before the authorities even realize a crime has been committed. One of the problems currently faced by investigators and prosecutors is that the evidence trail when a cybercrime has

occurred is difficult to establish. This is hampered by the fact that in a majority of countries, Internet Service or Content Providers are not obliged to retain data for any minimum period of time. This can mean that crucial data pointing towards the identification of a perpetrator is often lost.

Our law needs to respond to this. With the enactment of relevant legal provisions to ensure that internet service providers and internet content providers are obliged to keep data stored in their servers for a minimum period of time, this will bring us a step closer in being able to access the crucial evidence required to identify the perpetrators of these crimes and bring them to justice.

An increasing number of cybercrime investigations, including into cases involving child abuse and exploitation, require electronic evidence held by third parties. It is therefore critical that industry and Governments work together to develop mechanisms giving law enforcement timely access to data in emergency situations.

ii. The use of informal networks in order to facilitate international cooperation

We already have formal processes such as Mutual Legal Assistance and extradition that can be used to obtain evidence and assist investigations and apprehend fugitives but these processes can often be hampered by a variety of issues such as bureaucracy, issues of dual criminality and in some cases, lack of political will. In order to circumvent this, there also needs to be a reliance on informal international cooperation networks in order to ensure that we are able to obtain the evidence we need to prosecute cyber-criminals with as little obstacles as possible.

The G7 24/7 Cybercrime Network is one such example where the network is an informal one which aims to preserve data for transmission through formal channels like MLA as well as to be a Point to point network of established and knowledgeable personnel for urgent assistance in cybercrime matters. Brunei Darussalam is currently in the process of discussions to join the network. Such networking can bring about benefits in shaping investigations as well as shared expertise and experience in order to bring a successful conclusion to any investigation or prosecution. It must always be in our minds that criminals are not hampered by territorial borders or jurisdictional elements. As such, where we can and with the right political will, we can ensure that we are not impeded in our fight against cybercrime with such barriers.

iii. Information-Sharing

When dealing with cross-boundary crimes, it is essential in the implementation of any international cooperation mechanism that an understanding or a familiarization of the laws of the requested country be established before making any request for assistance. Within the China-ASEAN context, this is or will be no different. To address this, perhaps the CAPGC website can be utilised as a platform containing a database of all ASEAN Member States' and China's relevant laws and regulations in connection to cybercrime and international cooperation legal frameworks which prosecutors could easily refer to when considering international cooperation mechanisms.

To further facilitate this, a focal points database can also be developed where a focal point/officer is identified and appointed in each jurisdiction. This network of focal points will play the role of providing assistance that may be required by countries in understanding or familiarising themselves with the laws of that particular country. Whilst harmonisation of laws would be ideal, this would provide an alternative response in light of the inevitable

difficulties and challenges that would be encountered in any attempt to harmonise laws across different jurisdictions.

CONCLUSION

Excellencies, Distinguished Delegates, Ladies and Gentlemen,

We all know that the fight against cybercrime cannot be fought by one country alone, any success to be meted out will have to be the result of a unified stance at the regional and global level to enhance and continue efforts to stifle these criminal activities which deeply impacts governments and individuals anywhere around the world.

To this end, I hope that we will continue to use the China-ASEAN Prosecutors-General Conference as a platform to further strengthen our cooperation in our relentless efforts to combat transnational crime, especially cybercrime. I wish all of you a productive conference and look forward to hearing the methods your jurisdictions address cybercrime over the next few days. Thank you.