Speech to be delivered by Prof. Dr. Kennedy Gastorn, Secretary-General of AALCO at the Side Event on

"Enhancing International Cooperation in Combating Cyber Crime: An Asian-African Perspective"

to be held during the 9th Session of the Conference of Parties to the UNTOC, Vienna, Austria on 18 October 2018

Topic

"THE ROLE AND ACHIEVEMENTS OF AALCO IN PROMOTING INTERNATIONAL COOPERATION AGAINST CYBERCRIMES"

Outline

I. **Introduction**
II. **The Significance of International Cooperation to Counter the Perpetration of Cybercrimes**
III. **The Role and Achievements of AALCO in Promoting International Cooperation Against Cybercrimes**
IV. **Conclusion**

I. Introduction

Distinguished Panelists, Distinguished Delegates, Excellencies, Ladies and Gentlemen,

I warmly welcome you to this side event organized by Asian-African Legal Consultative Organization (AALCO). It is an honour and pleasure to speak as a Panelist today on the topic **"The Role and Achievements of AALCO in Promoting International Cooperation against Cybercrimes"**.

As you are already aware, AALCO is an intergovernmental organization which serves as a legal consultative and advisory body to its 47 Member States from Asia and Africa. This is the second time that we are organizing a side event in Vienna. Previously, we had organized a side event to the Twenty-Fifth Session of the Commission on Crime Prevention and Criminal Justice (CCPCJ) on 23 May 2016, on the topic "Cybercrimes and International Cooperation: An Asian-African Perspective". I heartily thank the Government of the People's Republic of China for providing financial and logistic support for organizing both the side events. I am also grateful to UNODC for giving us these opportunities.

Ladies and Gentlemen,

We are living in a digital global society where cybercrime is a global, transnational serious problem that needs strong technical and legal responses. In the absence of a universally accepted definition of cybercrime,[1] different definitions have been put forward by experts, the industry and scholars. Such definitions vary in their degree of specificity and breadth.[2]

One approach to cybercrimes is that they are just the digital edition of well-known, traditional offenses. Examples of "computerized or electronic" versions of traditional crimes contained in criminal codes are: fraud by using Information and Communications Technology (ICT) systems,

[1] Emilio C. Viano (2017), "Cybercrime: Definition, Typology, and Criminalization", in Emilio C. Viano (ed.), *Cybercrime, Organized Crime, and Societal Responses- International Approaches,* Switzerland: Springer International Publishing, 3-22, 3.
[2] Emilio C. Viano (2006), "Cybercrime: A new frontier in criminology", *International Annals of Criminology,* 44(1/2): 11-22, 11.

revelation of government secrets stored electronically, forgery of digitally stored data, defamation, stalking, or "cyber bullying".[3]

Other forms of ICT and cybercrime focus on interests that were not in existence before computers and other electronics were invented and the advent of the World Wide Web.[4] The acts of hacking and illegal monitoring are examples of this variety. The value of information as an asset today needs no emphasis. This asset is today exposed to continuous and virulent attacks conducted by cybercrime groups. This has called for allocation of significant financial and human resources to combat such menace.[5] Most probably, the largest challenge of criminal law in this century is to properly ascertain and determine the newly surfacing legal interests; defend them from inappropriate obstacles and clashes; and simultaneously determine the breadth of criminalization.[6]

It is noteworthy that at the national level, deterring cybercrimes has become an integral component of national cyber security and critical information infrastructure protection strategy.[7] In particular, this includes the adoption of appropriate legislation against the misuse of ICT for criminal or other illegal purposes and activities intended to affect the integrity of critical national infrastructures.[8] However, challenges are often posed and limits drawn to such legislation by, *inter alia,* the rapid pace of technological developments; conflicts with constitutional rights, e.g., the freedom of expressing one's opinion;[9] and the issues of sovereignty for crimes that take place in virtual environments. There ought to exist a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and the citizens.[10]

---

[3] S. W. Brenner and M. Rehber (2009), "'Kiddie Crime?' The utility of criminal law in controlling cyber-bullying", *First Amendment Law Review* 8(1): 1.
[4] *Supra* note 1 at 7.
[5] Victoria Stanciu and Andrei Tinca (2017), "Exploring cybercrime- realities and challenges", *Accounting and Management Information Systems*, 16 (4): 610- 632, 610.
[6] T. Eskola (2012), "From risk society to network society: Preventing cybercrimes in the 21st century", *Journal of Applied Security Research, 7*(1): 122-150, 122.
[7] Introductory Remarks Delivered by Prof. Dr. Rahmat Mohamad, Secretary-General of AALCO at the Side-Event on "Cyber Crimes and International Cooperation: An Asian-African Perspective" held during the 25th Session of CCPCJ, Vienna, Austria on 23 May 2016, in Yearbook of the Asian-African Legal Consultative Organization , Volume XIV (2016), 27- 31, 28.
[8] Ibid.
[9] *Supra* note 1 at 13-14.
[10] *Supra* note 7 at 28.

Cybercrime, both by definition and practice, transcends national borders. The interconnected nature of modern technology makes cybercrime a global problem, and for decades there has been international awareness of the need for coordinated action.[11] In broad terms, the global dimension of cybercrimes entails two legal repercussions. *Firstly*, jurisdiction issues are raised when there is the application of national laws to transnational conduct.[12] *Secondly*, and more pertinently from the viewpoint of the topic we have chosen for discussion today, it also makes international cooperation and harmonization in combating cybercrime an utmost necessity.

In view of this, prior to enunciating in detail the role and achievements of AALCO in promoting international cooperation against cybercrimes, I shall ponder, in brief, upon the importance of harmonization of the legal regimes countering cybercrimes and the significance of international and regional collaboration, coordination and cooperation to accomplish the objective of harmonization.

II. The Significance of International Cooperation to Counter the Perpetration of Cybercrimes

It is generally accepted that some degree of harmonization between countries is vital if effective regulation of cybercrimes is to be achieved. Although many offences are transnational in nature- for instance trafficking in humans, weapons and drugs, money laundering and terrorism- cybercrime presents unique challenges due to the inherently transnational nature of the underlying technology. No other type of crime can become transnational so effortlessly.

An attempt to decipher the rationale behind harmonization brings to the surface two reasons. In the words of Jonathan Clough,

> "The first is to eliminate or at least reduce the incidence of 'safe havens'. If conduct is not criminalised in a specific country, persons in that country may act

[11] Jonathan Clough (2014), "A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation", Monash U. L. Rev., 40: 698-736, 698.
[12] A. J. Colangelo (2011), "A unified approach to extraterritoriality", *Virginia Law Review*, 97: 1019.

> with impunity in committing offences that may affect other jurisdictions. Not only is there no ability to prosecute in the home jurisdiction, efforts at evidence gathering and extradition are likely to be thwarted in the absence of dual criminality. This raises the second and more far-reaching rationale; that harmonisation is crucial for effective cooperation between law enforcement agencies."[13]

Howsoever desirable, the idea of harmonization in this context is mired in considerable challenges. Each country brings its particular perspective, influenced by its legal tradition/s as well as cultural and historical factors. Addressing issues as complex and diverse as substantive and procedural law, mutual assistance and extradition pose significant difficulties. Even at the national level, issues of harmonization may accrue between state or provincial governments. In the international sphere, harmonization may be with other countries, regionally or internationally.[14] Although any international response to cybercrime must therefore seek to accommodate and reconcile these differences, it must be emphasized that "harmonized" does not mean "identical". The necessity of the hour is complementarity- enabling enforcement mechanisms to work effectively while respecting national and regional differences.

In order to spur the development of effective global norms and cooperation mechanisms to prosecute and punish perpetrators of cybercrimes, the UN General Assembly has adopted a series of resolutions. A number of legal instruments, some binding and some non-binding- notably the Council of Europe Conventions, the Shanghai Cooperation Organization Agreement, and the League of Arab States Convention, the Commonwealth Model Law, the Common Market for eastern and Southern Africa (COMESA) Draft Model Bill, the League of Arab States Model Law, and the ITU/CARICOM/CTU Model Legislative Texts- have been formulated. Even the most ambitious attempt to achieve harmonization, the product of over 16 years of preparatory work, the Council of Europe's Convention on Cybercrime (Budapest Convention) has been deemed to suffer from inadequacies. The Budapest Convention was the first multilateral binding instrument seeking to regulate cybercrime. Notably, AALCO Member States like Egypt, Nigeria and Pakistan have used the Convention as a model and drafted parts of their own legislation in

[13] *Supra* note 11 at 701.
[14] United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime" (Report, February 2013), 59-60.

accordance with it without formally acceding to it.[15] An international convention is, of course, only one approach to harmonization, and recent years have seen a flurry of activity in relation to cybercrime at the international, regional, national and organizational levels. I look forward to hearing my co-panelists' articulations on such activities in the Asian and African regions.

Combating cybercrime needs a comprehensive policy approach which takes note of cybercrime forecast trends in order to prevent new threats and to help ensure that adequate preparations are made in advance.[16] This prevention approach through threat assessments and strategic analysis ought to be complemented by outreach and international cooperation.[17] There is a clear need for them to establish dialogues at a vertical level (with prosecutors and judges) and at a horizontal level (with the internet industry, with other stakeholders and the civil society as a whole).[18]

III. The Role and Achievements of AALCO in Promoting International Cooperation Against Cybercrimes

Realization had dawned on many AALCO Member States in the past decade that effectively combating cybercrimes calls for enacting and enforcing comprehensive legislations. In tandem with national developments, AALCO Member States have joined various international and regional instruments aimed at countering the proliferation of cybercrimes and improving international cooperation for the harmonization of cyber-laws. However, differences between Member States regarding the mechanism for such harmonization still continue to persist. While some States advocate for the formulation of a comprehensive global convention, others are in favor of harmonizing domestic laws to the standards of existing international instruments.[19]

[15] Prof. Dr. Kennedy Gastorn (2017), "Relevance of International Law in Combating Cybercrimes: Current Issues and AALCO's Approach, Presentation at the 4th World Internet Conference, Wuzhen Summit, on the Session on "International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes", 4th December 2017, Wuzhen, China.
[16] Laviero Buono (2014), "Fighting cybercrime through prevention, outreach and awareness raising", *ERA Forum* 15:1-8.
[17] Ibid.
[18] Ibid.
[19] See for example, statements of Japan and People's Republic of China, Agenda Item: International Law in Cyberspace, Fifty Fourth Annual Session of AALCO, Beijing, 2015; Fifty Fifth Annual Session of AALCO, New Delhi, 2016; and Fifty Sixth Annual Session of AALCO, Nairobi, 2017.

There exists divergence of opinion vis-à-vis a more universal ratification of the Budapest Convention as well.

Recognizing *inter alia* the importance of intergovernmental deliberation to enhance cooperation in combating cybercrimes, People's Republic of China, in accordance with AALCO Statutory Rules, proposed "International Law in Cyberspace" as an agenda item to be deliberated at the Fifty-Third Annual Session of AALCO held in Tehran in 2014 and it was accepted by consensus. The Agenda Item was thereafter discussed at the Fifty-Fourth, Fifty-Fifth, Fifty-Sixth and Fifty-Seventh Annual Sessions, in 2015, 2016, 2017 and 2018 respectively. The resolution on the agenda item adopted in the 2015 AALCO Annual Session directed the Secretariat to study this subject based on deliberation and progress made in the UN framework and other forums, with special attention to, amongst others, rules of international cooperation in combating cybercrimes. A "Special Study" published by the Secretariat in 2017 has an exclusive chapter detailing the hitherto international efforts in addressing the menace of transnational cybercrime. As already noted, a Side Event on this topic of pertinence was organized in 2016 in Vienna.

Further, an Open-ended Working Group on International Law in Cyberspace was constituted in 2015 which met for the first time at the Fifty-Fifth Annual Session in 2016. The second meeting was held at the AALCO Headquarters in New Delhi in February, 2017. In that meeting, Dr. Huang Zhixiong, Rapporteur of the Working Group, remarked that regional and global instruments can certainly co-exist, and AALCO Member States should consider drafting Model Rules in this regard. Further, one of the Member States stressed upon the need to have a Model Law in place as regards rules of international law in combating cybercrimes, keeping in mind the best interest of all Member States.[20]

During the Fifty-Sixth Annual Session held in Nairobi, Kenya, in 2017 the topic International Law in Cyberspace was once again discussed by Member States, which was preceded by a Summary Report of the Chairperson of the Open-ended Working Group on International Law in Cyberspace, H.E. Mr. Hossein Panahi Azar, on the 2nd Working Group Meeting.

[20] *Supra* note 15.

Based on the mandate of the Fifty-Sixth Annual Session (2017),[21] Rapporteur of the AALCO Working Group on International Law in Cyberspace, Prof. Zhixiong Huang prepared a "Report on the Future Plan of Action of the Working Group Meeting", that was sent to all Member States by the Secretariat on 5 April 2018 for their comments and observations. Valuable comments on substantive parts of the Rapporteur's Report were received from some Member States, and the Report revised accordingly.[22]

The Third Meeting of the Open-ended Working Group on International Law in Cyberspace was held recently on 8 October 2018 with Mr. Abbas Bagherpour Ardekani, Head of Delegation, Islamic Republic of Iran as the Chairperson. The Rapporteur sought the AALCO Member States' cooperation in countering cybercrime. This suggestion was endorsed by a few Member States. Emphasizing the need for adoption of a set of model provisions, which will meet the need of AALCO Member States on preventing and combating cybercrime as well as contribute to the ongoing efforts in other international platforms sans any possibility of duplication or fragmentation of the regime, the Rapporteur welcomed inputs from all Member States of AALCO as to the basic framework and core elements of such model provisions.

In the recently concluded 57th Annual Session of AALCO in Tokyo, the role of international cooperation to combat cybercrimes was discussed whilst deliberating upon the agenda item "International Law in Cyberspace". Taking note of the Report of the Chairperson of the Working Group, the Member States proposed that the Working Group ought to continue to discuss the issue of international law in cyberspace with the aim to, *inter alia*, enhance cooperation in countering cybercrime. It was also decided that the Rapporteur prepare a report on the special need of the Member States for international cooperation against cybercrime.

Thus, AALCO has embarked on a quest to combat cybercrimes through international cooperation, and proposes to continue its deliberations and discussions in the future sessions.

[21] Resolution on "International Law in Cyberspace", AALCO/RES/DFT/56/S17, 5 May 2017.
[22] Substantive Brief International Law in Cyberspace, AALCO/57/TOKYO/2018/SD/S17 at http://www.aalco.int/userfiles/File/Final%20Brief%20of%20Cyberspace%202018.pdf

IV. Conclusion

It is alarming to note that, despite the all-pervading threat posed by cybercrimes, these crimes still do not command the attention, the concern, the prevention and the public education that crimes committed solely in real environment elicit in our society. In order to effectively combat cybercrimes, appropriate, interactive and dynamic legal framework at all levels- domestic, regional and international- ought to be chalked out fast. It is evident that the international community recognizes the significance of the harmonization of laws and facilitation of international cooperation in achieving global cyber security. Forms of international cooperation today include extradition, mutual legal assistance, mutual recognition of foreign judgments and informal police-to-police cooperation. However, there exist divergences in viewpoints regarding approaches of harmonization amongst nations. Two factors solicit mention in this context. *Firstly*, harmonization ought to be perceived as a process, not a destination. As the technology evolves and changes so too our responses will need to evolve and change. Rather than focusing on differences as an impediment to harmonization, the focus should be on how those differences may be resolved in working towards the common goal of effective international cooperation against a global challenge. *Secondly*, and as already noted, attempts at harmonization ought to accommodate and reconcile the extant differences, and hinge on the idea of complementarity, enabling enforcement mechanisms to work effectively while respecting national and regional differences. AALCO, as a multilateral forum representing such divergent interests and positions on the topic, holds immense potential for its Member States to be used as a platform to further deliberate on outstanding issues that come in the way of effective cooperation mechanisms.

Finally, awareness raising and continuous training are needed at all levels. Raising the overall awareness of the threat of cybercrime, especially among consumers and other vulnerable groups of potential victims, while avoiding undermining the trust of internet users by focusing exclusively on the potential dangers inherent in making use of the web, remains a key challenge for the years ahead. I must say that the UNODC and Council of Europe, as well as other regional and national initiatives have been playing an extremely valuable role in information sharing and capacity building. I ardently hope that our concerted efforts come to fruition, and we continue to combat cybercrimes via cooperation and collaboration.

Thank you.