

AALCO/57/TOKYO/2018/SD/S17

For official use only

ASIAN-AFRICAN LEGAL CONSULTATIVE ORGANIZATION



INTERNATIONAL LAW IN CYBERSPACE

**Prepared by
The AALCO Secretariat
29 C, Rizal Marg,
Diplomatic Enclave, Chanakyapuri,
New Delhi – 110 021
India**

CONTENTS

I. Introduction	1-3
A. Background	
B. Issues for focused deliberation at the Current Annual Session	
II. Annexures	4-51
A. Annexure 1: Report on the Future Plan of Action of the Working Group by Prof. Zhixiong Huang, Rapporteur of the AALCO Working Group on International Law in Cyberspace	
B. Annexure 2: Comments by the Islamic Republic of Iran on the “Report on the Future Plan of Action of AALCO’s Working Group on International Law in Cyberspace”	
C. Annexure 3: Comments of People’s Republic of China on the “Future Plan of Action of the Working Group”	
D. Annexure 4: Comments by Japan on draft “Report on the Future Plan of Action of the Working Group Meeting”	
E. Annexure 5: Report on the Future Plan of Action of the Working Group Meeting by Prof. Zhixiong Huang, Rapporteur of the AALCO Working Group on International Law in Cyberspace (revised)	
F. Annexure 6: Comments by Islamic Republic of Pakistan on “Report on the Future Plan of Action of the Working Group Meeting”	

I. Introduction

A. Background

1. Taking note of the enormous international discussions and developments in the field of cyberspace as well as the glaring challenges posed by it which were encountered by States on a day-to-day basis, People's Republic of China, in accordance with the Statutory Rules of AALCO, had proposed the topic "International Law in Cyberspace" as an agenda item for the Fifty-Third Annual Session of AALCO, that was held in Tehran (Iran) in 2014, and which was accepted as such by consensus.
2. This agenda item was thereafter deliberated subsequently in the Fifty-fourth Annual Session held in Beijing, China in April 2015, during which the Member States decided to establish an Open-ended Working Group on International Law in Cyberspace to further discuss the matter through meetings or workshops to be cosponsored with Governments of the Member States or relevant international organizations.¹
3. During the First Meeting of AALCO Working Group on International Law in Cyberspace convened in New Delhi during the Fifty-Fifth Annual Session of AALCO on 19 May 2016, which was chaired by H.E. Mr. Hossein Panahi Azar, then Director General for International Legal Affairs, Ministry of Foreign Affairs, Islamic Republic of Iran, delegates addressed some important issues such as applicability of international law in cyberspace, the domestic legal framework, State sovereignty in cyberspace, rules of international cooperation in combating cybercrimes, and future work of the Working Group. The resolution adopted at that Annual Session firstly encouraged Member States to actively participate in relevant regional and global fora deliberating on the governance of cyberspace and to strengthen their communication and cooperation in this regard; secondly, directed the Working Group to hold inter-sessional meetings, preferably in cooperation with Member States and relevant international organizations and other institutions, in pursuance of its mandate; and also further directed the Secretariat to closely follow the developments in international forums related to governance of cyberspace and cyber security.² Prof. Zhixiong Huang of Wuhan University Law School of the People's Republic of China was elected the Rapporteur of the Working Group in this meeting.
4. The second meeting of the Open-ended Working Group on International Law in Cyberspace took place at the AALCO Headquarters in New Delhi, from 9-10 February 2017. 23 Member States of AALCO participated in the meeting.³ Six sessions were held

¹ Resolution on "International Law in Cyberspace", AALCO/RES/DFT/54/S17, 17 April 2015.

² Resolution on "International Law in Cyberspace", AALCO/RES/DFT/55/S17, 20 May 2016.

³ Arab Republic of Egypt, People's Republic of China, Cyprus, Democratic People's Republic of Korea, India, Indonesia, Islamic Republic of Iran, Japan, Malaysia, Mongolia, Myanmar, Nepal, Sultanate of Oman, State of Qatar, Kingdom of Saudi Arabia, South Africa, Sri Lanka, State of Palestine, Tanzania, Sudan, Syrian Arab Republic, Thailand and Republic of Yemen. See, Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.137

during the 2-day meeting. The sessions dealt with four substantive topics: a) Sovereignty in Cyberspace: Balancing Rights and Obligations, b) Law and Governance of Cyberspace, c) Cyber Warfare: Legal Implications, and d) Cybercrimes and International Law. At the concluding session of the meeting AALCO Secretariat presented an introduction to the “Special Study on International Law in Cyberspace”, which was to be released at the upcoming Fifty-Sixth Annual Session. Member States also had the opportunity to discuss the future work of the Working Group.

5. 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. Further, the AALCO Secretariat’s Special Study on International Law in Cyberspace, based on the mandates received at the Fifty-Fourth and Fifty-Fifth Annual Sessions, was released at this Annual Session.⁴ Till this time the topic International Law in Cyberspace had already been discussed over four sessions at AALCO, including two Working Group Meetings. Based on those discussions, the Special Study focused upon and covered 5 substantive topics: a) Cyberspace: Its Nature and Characteristics; b) State Sovereignty in Cyberspace: Rights and Obligations; c) International Law and Governance of Cyberspace; d) Cyber Warfare and International Law; and e) Cybercrimes: International Legal Responses. The resolution adopted during the Annual Session, *inter alia*, directed the Rapporteur of the Open-ended Working Group on International Law in Cyberspace to prepare a Report on the basis of the discussions that have taken place thus far among the Member States, and the Special Study prepared by the Secretariat, laying down a future plan of action for the Working Group.⁵
6. Based on this mandate, 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. The Report is divided into three parts: a) Development of International Law in Cyberspace; b) Progresses within AALCO so far; and c) Suggestions as to the Future Plan of Action of the Working Group. Comments on the Rapporteur’s Report were received from 3 Member States:

⁴ The Resolution adopted at the 54th Annual Session of AALCO in 2015 directed the Secretariat to study the subject of “International Law in Cyberspace, based on deliberation and progress made in the UN framework and other forums, with special attention to international law pertaining to State Sovereignty in cyberspace, peaceful use of cyberspace, rules of international cooperation in combating cybercrimes, and identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace”. The resolution adopted at the 2016 Annual Session pursuant to the deliberations in the first meeting of the Open-ended Working Group on International Law in Cyberspace, further directed the Secretariat to closely follow developments in international forum related to governance in cyberspace and cyber security and continue its study on International Law in cyberspace which began in 2015, with a view to assisting the Working Group to fulfil its mandate. Bearing in mind these mandates the Secretariat came up with the present Study, which is based on the broad framework as laid down in the afore-stated resolutions.

⁵ Resolution on “International Law in Cyberspace”, AALCO/RES/DFT/56/S17, 5 May 2017.

Islamic Republic of Iran, People's Republic of China, and Japan within the month of June 2018. These comments made valuable suggestions on the substantive parts of the Report. Based on these comments a revised Report by the Rapporteur was again sent to all Member States on 6 August 2018 for their comments and observations. On the basis of the revised Report, the Islamic Republic of Pakistan submitted its comments on 30 August, 2018.

B. Issues for focused deliberation at the Current Annual Session

- 1) Report on the Future Plan of Action of the Working Group by Prof. Zhixiong Huang, Rapporteur of the AALCO Working Group on International Law in Cyberspace
- 2) Comments and Observations of the Member States on the Rapporteur's Report
- 3) Future Plan of Action of the Working Group based on the discussions in the third meeting of the Open-ended Working Group on International Law in Cyberspace

Annexure 1

Asian-African Legal Consultative Organization Working Group on International Law in Cyberspace

Report on the Future Plan of Action of the Working Group

Zhixiong Huang*, Rapporteur of the
AALCO Working Group on International Law in Cyberspace

1. The Asian-African Legal Consultative Organization (hereinafter referred to as “AALCO”) adopted Resolution AALCO/RES/56/S 17 at its Fifty-Sixth Annual Session on 5 May 2017 which, among others, “directs the Rapporteur of the Open-ended Working Group on International Law in Cyberspace (hereinafter referred to as “the Working Group”) to prepare a Report on the basis of the discussions that have taken place thus far among the Member States, and the Special Study prepared by the Secretariat, laying down a future plan of action for the Working Group.” This Report, drafted pursuant to that mandate, is divided into three parts: (I) Development of International Law in Cyberspace; (II) Progresses within AALCO so far; (III) Suggestions as to the Future Plan of Action of the Working Group.

I. Development of International Law in Cyberspace

2. It has been generally agreed that the sui generis character of cyberspace does not preclude it from regulation of existing rules and principles of international law, and that the fundamental tenet of international law, i.e. state sovereignty is intrinsically linked with internet governance.¹ In the meantime, there is also a consensus that “[g]iven the unique attributes of ICTs, additional norms could be

* LuoJia Chair Professor and Vice Dean, Law School of Wuhan University, China.

¹ International Law in Cyberspace, AALCO/54/BEIJING/2015, para.4.

developed over time”.² Currently, a number of international institutions and processes have touched on the issues related to the development and application of international rules, among which, the following two platforms within the framework of the United Nations are particularly noteworthy.

3. Consisting of representatives from the 5 permanent members of the United Nations Security Council and other 10-20 States, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter referred to as “GGE”) has been regarded as one of the most influential inter-governmental mechanisms exploring possible consensus on application and development of international rules for cyberspace. In June 2013, a consensual final report adopted by the 3rd GGE (2012-2013) confirmed that “[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment”.³ In June 2015, the 4th GGE (2014-2015) adopted a new consensual final report, which proposed 11 paragraphs on voluntary, non-binding norms, rules or principles of responsible behavior of States, as well as 6 paragraphs on how international law applies to the use of ICTs by States.⁴ However, due mainly to controversies over specific issues regarding the application of certain rules of international law (e.g. the right to self-defense, international humanitarian law, and state responsibility) to cyberspace, the 5th GGE (2016-2017) comprised of 25 States failed to reach a new final report.⁵

4. In the area of combating cybercrime, the UN General Assembly, in its resolution 65/230 in 2010, requested the Commission on Crime Prevention and Criminal Justice (hereinafter referred to as “CCPCJ”) to establish an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of

² See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para. 16; United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 15.

³ See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para. 11, paras. 19-20.

⁴ See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 13, para. 28.

⁵ See UNODA, Developments in the Field of Information and Telecommunications in the Context of International Security, <https://www.un.org/disarmament/topics/informationsecurity>.

cybercrime and responses to it by Member States, the international community and the private sector, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime (hereinafter referred to as “IEG”).⁶ The first session of the IEG was held in Vienna from 17 to 21 January 2011. At that session, the IEG reviewed and adopted a collection of topics and a methodology for the study. In its resolution 67/189, the General Assembly noted with appreciation the work of the IEG and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the CCPCJ in due course. The second session of the IEG was held from 25 to 28 February 2013. At that session, the IEG, inter alia, took note of the *draft comprehensive study of the problem of cybercrime*⁷ and responses to it by Member States, the international community and the private sector, as prepared by the United Nations Office on Drugs and Crime (UNODC) under the auspices of the IEG, pursuant to the mandate contained in General Assembly resolution 65/230. This draft study offered several options to strengthen existing and to propose new national and international legal or other responses to cybercrime, including the development of international model provisions; development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters; development of a comprehensive multilateral instrument on cybercrime; and delivery of enhanced technical assistance for the prevention and combating of cybercrime in developing countries. The third session of the IEG took place in Vienna from 10 to 13 April 2017. Based on the recommendations of the third session, the CCPCJ in its resolution 26/4 requests the IEG to continue its work and, in so doing, to hold periodic meetings and function as the platform for further discussion on substantive issues concerning cybercrime.⁸

⁶ <http://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html>

⁷ The methodology for the study tasked the United Nations Office on Drugs and Crime with developing the study, including developing a questionnaire for the purposes of information gathering, collecting and analyzing data, and developing a draft text of the study. Information gathering in accordance with the methodology, including the distribution of a questionnaire to Member States, intergovernmental organizations and representatives from the private sector and academic institutions, was conducted by UNODC, from February 2012 to July 2012. Information was received from 69 Member States with regional distribution as follows: Africa (11), Americas (13), Asia (19), Europe (24), and Oceania (2). Information was received from 40 private sector organizations, 16 academic organizations and 11 intergovernmental organizations. Over 500 open source documents were also reviewed by the Secretariat. This draft study offered several options to strengthen existing and to propose new national and international legal or other responses to cybercrime, including the development of international model provisions; development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters; development of a comprehensive multilateral instrument on cybercrime; and delivery of enhanced technical assistance for the prevention and combating of cybercrime in developing countries.

⁸ Report on the meeting of the Open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 10 to 13 April 2017, UNODC/CCPCJ/EG.4/2017/4; The Commission on Crime Prevention and Criminal Justice, Strengthening international cooperation to combat cybercrime, Resolution

Pursuant to the above CCPCJ resolution and aims to facilitate its implementation, the Chair of IEG proposed the 2018–2021 work plan⁹ of the IEG recently and will be adopted at the forthcoming 4th IEG meeting to be held in 3-5 April 2018. It is expected that the IEG will be a main forum for international rules-making on combating cybercrime in the coming years.

5. It is also noteworthy that Russian Federation recently submitted a *Draft United Nations Convention on Cooperation in Combating Information Crimes* to the United Nations General Assembly as an UN official document (A/C.3/72/12). It is the first suggestion on a global Convention on cybercrime to the UNGA by a state.

II. Progresses within the Framework of AALCO so far

6. Based on the recommendation of the People's Republic of China, Member States of AALCO agreed to incorporate the topic "International Law in Cyberspace" as a regular agenda item at the Fifty-third Annual Session in Tehran, Iran in September 2014.¹⁰ This agenda item was also deliberated in the Fifty-fourth Annual Session held in Beijing, China in April 2015, during which the Member States decided to establish an Open-ended Working Group on International Law in Cyberspace to further discuss the matter through meetings or workshops to be cosponsored with Governments of the Member States or relevant international organizations.¹¹

7. In the First Meeting of AALCO Working Group on International Law in Cyberspace convened in New Delhi during the Fifty-Fifth Annual Session of AALCO on 19 May 2016, H.E. Mr. Hossein Panahi Azar, then Director General for International Legal Affairs, Ministry of Foreign Affairs, Islamic Republic of Iran, H.E. Ms. Njeri Mwangi Wachira, Chief State Counsel, Kenya, and Prof. Zhixiong Huang of Wuhan University Law School of the People's Republic of China, were

26/4,

http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCPCJ_Res_Dec/CCPCJ-R ES-26-4.pdf

⁹ Main topics for 2018-2020 meetings including: Legislation & frameworks;Criminalization; Law enforcement & investigations;Electronic evidence & criminal justice;International cooperation;Prevention. No later than 2021,the IEG will hold stock-taking meeting that will finish consideration of all the preliminary conclusions and recommendations and will produce a consolidated list of adopted conclusions and recommendations for submission to the CCPCJ,

<http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/V1800915.pdf>.

¹⁰ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/53/S17, 18 SEPTEMBER 2014.

¹¹ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/DFT/54/S17, 17 APRIL 2015.

respectively elected as the Chairperson, Vice-Chairperson and Rapporteur of the Working Group. During the meeting, delegates addressed some important issues such as applicability of international law in cyberspace, the domestic legal framework, State sovereignty in cyberspace, rules of international cooperation in combating cybercrimes, and future work of the Working Group. A resolution adopted at that Annual Session encourages Member States to actively participate in relevant regional and global fora deliberating on the governance of cyberspace and to strengthen their communication and cooperation in this regard; directs the Working Group to hold inter-sessional meetings, preferably in cooperation with Member States and relevant international organizations and other institutions, in pursuance of its mandate; and also directs the Secretariat to closely follow the developments in international forums related to governance of cyberspace and cyber security.¹²

8. During 9-10 February 2017, the second meeting of the Open-ended Working Group on International Law in Cyberspace was convened at AALCO Headquarters in New Delhi. 23 Member States of AALCO participated in the meeting.¹³ Six sessions were held during the 2-day meeting. The inaugural session comprised of addresses by the Secretary General of AALCO Prof. Kennedy Gastorn, the President of the Fifty-Fifth Annual Session of AALCO Dr. V.D. Sharma, and the Chairperson of the Working Group Mr. Hossein Panahi Azar on the present day importance of the topic, “International Law in Cyberspace” and the continued relevance of the Working Group respectively. The next four sessions dealt with four major areas: State sovereignty in cyberspace, law and governance of cyberspace, cyber warfare, and cybercrimes and international law. Three experts Mr. Arun Mohan Sukumar, Head, Cyber Initiative, Observer Research Foundation, Mr. Jeremy England, Head of ICRC in New Delhi and Dr. Zhixiong Huang, Professor, Wuhan University Law School of the People’s Republic of China, and the Rapporteur of the Working Group, as guest speakers, gave their introductory speeches on sovereignty in cyberspace, cyber warfare and cybercrimes respectively, Member States presented their statements and had interactions with the experts. In the concluding session, the Secretariat briefly

¹² RESOLUTION ON “INTERNATIONAL LAW IN CYBERSPACE”, AALCO/RES/DFT/55/S17, 20 MAY 2016.

¹³ Arab Republic of Egypt, People’s Republic of China, Cyprus, Democratic People’s Republic of Korea, India, Indonesia, Islamic Republic of Iran, Japan, Malaysia, Mongolia, Myanmar, Nepal, Sultanate of Oman, State of Qatar, Kingdom of Saudi Arabia, South Africa, Sri Lanka, State of Palestine, Tanzania, Sudan, Syrian Arab Republic, Thailand and Republic of Yemen. See, Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.137

introduced the content of its Special Study on international law in cyberspace which will be released in the coming Annual Session of AALCO. Member States also had the opportunity to discuss the future work of the Working Group, the suggestion of having a Model Law in place as regards rules of international law in combating cybercrimes was proposed.¹⁴

9. On 5 May 2017, the topic of international law in cyberspace was discussed by AALCO Member States during the Fifty-Sixth Annual Session held in Nairobi, Kenya, preceded by a Summary Report of the Chairperson of the Open-ended Working Group on International Law in Cyberspace, on the 2nd Working Group Meeting. Several issues, of which the state sovereignty and fundamental human rights in cyberspace, Internet governance, international cooperation in combating cybercrime, law of armed conflict and state responsibility in cyberspace, etc, were discussed. Member States recognized the imperative role of AALCO in promoting Member States to share insights and reach consensus on the issues mentioned above.¹⁵ The resolution adopted during the Annual Session, inter alia, directed the Rapporteur of the Open-ended Working Group on International Law in Cyberspace to prepare a Report on the basis of the discussions that have taken place thus far among the Member States, and the Special Study prepared by the Secretariat, laying down a future plan of action for the Working Group.¹⁶

10. Thus far, discussions among AALCO Member States have focused on the following topics: international law pertaining to State Sovereignty in cyberspace, peaceful use of cyberspace, rules of international cooperation in combating cybercrimes, identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace and law and governance of Cyberspace, etc.¹⁷ On international law pertaining to State Sovereignty in cyberspace, while many countries, by invoking the consensus reached by the GGE,¹⁸ reaffirmed the

¹⁴ Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, pp.137-139.

¹⁵ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.143, p.145.

¹⁶ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/DFT/56/S17, 5 MAY 2017.

¹⁷ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/DFT/54/S17, 17 APRIL 2015.

¹⁸ United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para. 20; United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 27.

application of the principle of State Sovereignty in cyberspace, they also concerned with the questions such as the exercise of extra-territorial criminal jurisdiction,¹⁹ data based jurisdiction,²⁰ and the need to strike a proper balance between sovereign rights in cyberspace and the protection of fundamental human rights, such as freedom of expression and confidentiality of communication.²¹ On the peaceful use of cyberspace, Member States mainly concerned about the escalation in militarization of the cyberspace,²² and clarification of the standards for legal attribution of cyber activities to a state.²³ Some Member States pointed out that under some circumstances, cyber activities could amount to the use of force or an armed attack within the context of UN Charter and customary international law.²⁴ While others cautioned that many elements pertaining to this issue remain open to discussion, and stressed that no abuse may be tolerated in resort to force or self-defense, and the sanctity of article 2(4) of the UN Charter must remain intact in all circumstances.²⁵ On the rules of international cooperation in combating cybercrimes, some Member States underscored the importance of the Convention on Cybercrime of the Council of Europe (or the Budapest Convention), emphasized that appropriate consideration should be given so as not to duplicate the efforts by creating something very similar to the Budapest Convention.²⁶ Some other Members criticized the Budapest Convention as being fundamentally unbalanced and questioned its legitimacy and long-effectiveness.²⁷ The need to have a multilateral treaty that would effectively prevents escalation of cybercrime, preferably through a UN-centric governance model

¹⁹ See, e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.166.

²⁰ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.144.

²¹ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.188; Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.165.

²² See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.81.

²³ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.145.

²⁴ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.151.

²⁵ See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, pp.166-167; Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.151 and p.148.

²⁶ See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, pp.165.

²⁷ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.187 and Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.167.

for cyberspace, was clearly supported by some Member States.²⁸ On the identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace, some Member States stated that the unique characteristics of network technology necessitate a renewed debate and considered international effort to develop the criteria that would determine the application of international law and principles to cyberspace, since the current legal framework is not enough to provide solutions to the security dilemma posed by cyberspace.²⁹ Other Members also pointed to the fact that cyberspace remains a domain which lacks of substantial rules and regulations due to its intangibility, and highlighted the need to step up our efforts to develop and promote the norms, rules and principles to be applied to cyberspace.³⁰ On the law and governance of cyberspace, Member States introduced and reviewed latest progresses made in their domestic cyber policies, legislation and institution development. While some in support of a multi-stakeholder approach that neither the government nor the industry has the monopolistic dominance over one another,³¹ others in support of a multilateral management of the Internet whereby United Nations serves as the main channel in promoting the adoption of accepted international rules in cyberspace, and all states would have a share in the regulation and management of the Internet.³² Some even called on AALCO to adopt of its resolution to prepare an international convention for the regulation of cyberspace in order to ensure the use of cyberspace for the service of mankind.³³

11. AALCO Secretariat, pursuant to the relevant mandate by Member States, has been closely following developments in international forums related to governance of cyberspace and cyber security. Besides the Open-ended Working Group meetings organized by the Secretariat mentioned above, it also organized, with the financial and logistical support from the Government of People's Republic of China, a side event on

²⁸ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.181.

²⁹ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.88 and p.190.

³⁰ Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.143.

³¹ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.145.

³² See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.162 and Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/Nairobi/2017/VR, p.141.

³³ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.193.

the theme “Enhancing International Cooperation on Combating Cybercrimes” during the 25th session of CCPCJ on 23 May 2016 at the UN Office in Vienna, Austria.³⁴ On the invitation from the Chinese Ministry of Foreign Affairs to AALCO, the Secretary-General of AALCO attended the 4th World Internet Conference (WIC) held at Wuzhen International Internet Exhibition and Convention Center in Wuzhen, China from 3-5 December, 2017. The Secretary-General presented a paper on “Relevance of International Law in Combating Cybercrime: Current Issues and AALCO’s Approach” at the session on “International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes”. Moreover, mandated by the resolution adopted at the Fifty-Fourth Annual Session, AALCO Secretariat prepared a Special Study on International Law in Cyberspace,³⁵ which was released during the Fifth-Sixth Annual Session held in Nairobi, Kenya in May 2017.

12. In short, AALCO Member States have stressed the significance of the principles and rules of international law applicable to cyberspace, including those in the UN Charter, and the need for further study, discussion and development of rules of international law on cyberspace issues.³⁶ In particular, the importance of international cooperation in combating cybercrime has been frequently stressed in previous discussions in AALCO. For example, the resolution adopted by AALCO Member States mandated the Working Group “to hold inter-sessional meetings, preferably in cooperation with Member States and relevant international organizations and other institutions in particular the United Nations in pursuance of its mandate, *taking into account the need of AALCO Member States in combating cybercrime*” (emphasis added).³⁷ It also underlined the need for enhanced coordination and judicial cooperation among Member States in combating the criminal misuse of information and communication technologies.³⁸

III. Suggestions as to the Future Plan of Action of the Working Group

13. The unique attributes of cyberspace have raised a number of important legal

³⁴ AALCO’s Side Event “Enhancing International Cooperation on Combating Cybercrimes” was Held in Vienna, <http://www.aalco.int/Side%20Event.pdf>

³⁵ AALCO Secretariat, *International Law in Cyberspace*, New Delhi, 2017.

³⁶ See, e.g., RESOLUTION ON “INTERNATIONAL LAW IN CYBERSPACE”, AALCO/RES/DFT/56/S17, 5 MAY 2017.

³⁷ RESOLUTION ON “INTERNATIONAL LAW IN CYBERSPACE”, AALCO/RES/DFT/55/S17, 20 MAY 2016.

³⁸ *Id.*

challenges relating to the application of international law in cyberspace.³⁹ On the basis of the discussions that have taken place thus far among the Member States and studies conducted by the Secretariat, the following suggestions are offered for consideration of a future plan of action of the Working Group.

A. Enhancing AALCO Member States' cooperation in countering cybercrime

14. Cybercrime is now a global threat. According to the Global Risks Report 2016, global cost of cybercrime will reach \$ 2 trillion by 2019, a threefold increase from the 2015 estimate of \$ 500 billion.⁴⁰ Because of the transnational nature of cybercrime, international cooperation in extradition, mutual legal assistance, mutual recognition of foreign^[SEP] judgments, and police-to-police cooperation, are essential. Yet, a prominent feature of international cooperation in this area is fragmentation at the international level, and diversity of national cybercrime laws.⁴¹ In order to effectively combat cybercrime, the existing instruments and mechanisms must be harmonized and improved. This is why some Member States who are already Contracting Parties to one or several existing instruments stressed the need for a global comprehensive instrument pertaining to cybercrime.⁴² As such, some delegations called upon AALCO Secretariat to conduct a detailed study on the appropriate rules of international cooperation in combating cybercrime which may thereafter lead to the formation of a guideline in this aspect.⁴³ Besides, the Chairperson's Summary Report of the 2nd Meeting of Open-ended Working Group on International Law in Cyberspace proposed that, the future work priority and outcome of the Working Group could be the prospective AALCO guidelines or model provisions on cyberspace.⁴⁴ One of the important concrete conclusions in the Special Study on International Law in Cyberspace prepared by AALCO Secretariat is that it is

³⁹ See e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/Nairobi/2017/VR, p.144.

⁴⁰ See *Global Risks Report 2016*, <http://reports.weforum.org/global-risks-2016/>

⁴¹ Currently there are several regional initiatives in combating cybercrime, including the 2001 Convention on Cybercrime of the Council of Europe (also known as the Budapest Convention), the 2010 League of Arab States Convention on Combating Information Technology Offenses, the 2001 Commonwealth of Independent States Agreement on Cooperation in Combating Offenses related to Computer Information, the 2010 Shanghai Cooperation Organization Agreement in the Field of International Information Security, and the African Union Convention on Cybersecurity and Personal Data Protection.

⁴² See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.98.

⁴³ See Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.167.

⁴⁴ Chairperson's Summary Report of the 2nd Meeting of Open-ended Working Group on International Law in Cyberspace, <http://www.aalco.int/Working%20Group%20Report%202017.pdf>.

important for nations to come together to work on uniform rules of international law for curbing cyber-crimes.⁴⁵ It also follows with the last sentence of the Study states: “It has brought out the glaring defect that till now cyber-crimes have been regulated haphazardly and in piecemeal fashion, with there being national legislations, and many binding as well as non-binding regional and international instruments regulating cybercrimes, with overlapping or even sometimes conflicting provisions.”

15. In past decades, AALCO Member States already gained extensive experience in drafting principles or model articles on issues such as extradition of fugitive offenders,⁴⁶ admission and treatment of aliens,⁴⁷ elimination or reduction of dual or multiple nationality,⁴⁸ and promotion and protection of investment.⁴⁹ These principles and draft articles have played an important role in deepening discussions and forging consensus among AALCO Member States.

16. From the above, it may be fair to say that drafting a set of model provisions on preventing and combating cybercrime within the framework of AALCO could serve as a useful first step for the future work of the Working Group. The drafting process may operate in the following steps: first, all Member States of AALCO will be invited to submit written comments on the basic framework and core elements of the Model Provisions. Second, with the assistance of AALCO Secretariat, the Rapporteur of the Working Group may be mandated to prepare, based on the written submissions of the Member States of AALCO, a Draft Model Provisions for the consideration of Working Group. Third, the Working Group will be mandated to formulate, based on the Draft of the Rapporteur, a Model Provisions to be adopted by AALCO Annual Session.

B. Deepening discussions on some key issues of international law in cyberspace among AALCO Member States

17. Setting up crosscutting sub-topics. Four topics, i.e. sovereignty in

⁴⁵ AALCO Secretariat, International Law in Cyberspace, New Delhi, 2017, pp.112-113.

⁴⁶ ARTICLES CONTAINING THE PRINCIPLES CONCERNING EXTRADITION OF FUGITIVE OFFENDERS,
<http://www.aalco.int/ARTICLES%20CONTAINING%20THE%20PRINCIPLES%20CONCERNING%20EXTRA%20DITION%20OF%20FUGITIVE%20OFFENDERS.pdf>.

⁴⁷ PRINCIPLES CONCERNING ADMISSION AND TREATMENT OF ALIENS,
<http://www.aalco.int/PRINCIPLES%20CONCERNING%20ADMISSION%20AND%20TREATMENT%20OF%20ALIENS.pdf>

⁴⁸ MODEL ARTICLES EMBODYING PRINCIPLES RELATING TO ELIMINATION OR REDUCTION OF DUAL OR MULTIPLE NATIONALITY,
<http://www.aalco.int/Model%20Articles%20Embodying%20Principles.pdf>.

⁴⁹ PROMOTION AND PROTECTION OF INVESTMENTS,
<http://www.aalco.int/PROMOTION%20AND%20PROTECTION%20OF%20INVESTMENTS.pdf>.

cyberspace, peaceful use of cyberspace, international cooperation on combating cybercrime and the application and development of existing instruments, have been included in the agenda items of the Working Group. In order to facilitate further discussions among AALCO Member States on these topics, sub-topics on crosscutting issues such as sovereignty on data and equal participation in international governance of the Internet under the topic of sovereignty in cyberspace, or digital evidence and trans-boundary data collecting under the topic of international cooperation on combating cybercrime may be set up. They can be designated before each meeting of the Working Group, with the aim of facilitating in-depth discussions.

18. Conducting research on terminology. In order to promote common understandings among AALCO Member States on the key issues of international law in cyberspace, it's helpful for the Member States, with the support of the Secretariat and the Rapporteur of the Working Group, to conduct research on such key terms as hacker attack, cyber warfare, cybercrime, cyber terrorism, governance of cyberspace (or Internet governance), Internet surveillance, critical cyber infrastructure, etc. In the end, a list of terms can be published.⁵⁰

19. Adding new topics where appropriate. In accordance with the new development in international law in cyberspace and the practical needs of AALCO Member States, new topics beyond those four existing topics such as international rules on digital economy may be added to the agenda items.

C. Strengthening capacity building in AALCO

20. Information-gathering and research by the Secretariat. The Secretariat may engage in further information gathering and research on all existing and future topics of the Working Group, so as to provide useful support to the discussion of those topics by the Working Group.

21. Establishing platforms for information-sharing. With the support and involvement of AALCO Member States, the Secretariat may upload relevant legislations and policy documents of the Member States and new achievements

⁵⁰ It's noteworthy that in view of the importance of such terms, the International Telecommunication Union (ITU), The Internet Corporation for Assigned Names and Numbers (ICANN), the National Institute of Standards and Technology (NIST) of the United States have already published (and periodically updated) definitions of cyber-related terms. The NATO think tank CCD COE also compiles and researches the terms relating to cyber security. See, e.g. Glossary of ICANN, <https://www.icann.org/resources/pages/glossary-2014-02-03-en>; Glossary of Key Information Security Terms, NIST, <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>; Cyber Definitions of NATO Cooperative Cyber Defence Center of Excellency, <https://ccdcoe.org/cyber-definitions.html>.

relating to international legislations to the official website of AALCO, which could be an invaluable platform for information-sharing among the Member States.

22. Carrying out international exchange and cooperation program. Close cooperation on concrete program between AALCO Member States and the Secretariat should be encouraged and further explored through joint effort by the Secretariat and Member States. One latest example is an international seminar on combating cybercrime held by the Chinese government in cooperation with AALCO during the 3rd Training Session of the China-AALCO Exchange and Research Program in International Law in September 2017. Organization of similar events should be encouraged in the future.

**Comments by the Islamic Republic of Iran
on “The Report on the Future Plan of Action of AALCO’s Working Group on
International Law in Cyberspace”**

3 June 2018

1. Pursuant to Resolution AALCO/RES/56/S 17 at the Fifty-Sixth Annual Session on 5 May 2017, Mr. Zhixiong Huang, as the Rapporteur of the Open-ended Working Group on International Law in Cyberspace was directed to prepare a Report on the basis of the discussions held by the Member States. In this regard, the plan of action proposed in the Special Study as prepared by the Secretariat sets out three areas on which the work of the Rapporteur would focus, namely (I) Development of International Law in Cyberspace (2) Progresses within AALCO (III) Suggestions as to the Future Plan of Action of the Working Group. Our comments will be based thereon.
2. On the “Development of International law in Cyberspace”, we concur with the Rapporteur that ‘the sui generis character of cyberspace does not preclude it from regulation of existing rules and principles of international law’. Diverse issues currently under discussion in international law in Cyberspace ranging from internet governance to international humanitarian law and cybercrimes do remain within the ambit of the existing principles and rules of international law. Basic tenets of international law including State sovereignty, equality of States and prohibition of threat or use of force remain to be the cornerstones of any framework regulating any of the famous five domains especially cyberspace. It is against such a background that the Islamic Republic of Iran follows the ongoing work of the international institutions and processes including that of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) and that of the open-ended intergovernmental expert group established at the request of the Commission on Crime Prevention and Criminal Justice (CCPCJ). It remains to be highlighted, however, that the intricacies and complexities of the Cyberspace still require further regulation at the international level, which is to be developed based on the existing principles of international law and to which, we believe, AALCO could make important contributions.
3. We understand that progress in the work of the existing initiatives within the United Nations and elsewhere highly depends on such controversial and complex issues as the application of certain rules of international law to cyberspace, and new national and international legal or other responses to cybercrime, including the development of

international model provisions, development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters, development of a comprehensive multilateral instrument on cybercrime, and delivery of enhanced technical assistance for the prevention and combating of cybercrime in developing countries. Some international law concepts which appear to be crystal clear in other areas still remain in the gray zone of international law when it comes to Cyberspace and there's little consensus on their exact definition and application at the international level. Use of force in Cyberspace, its contours and the right to self-defense, applicability and application of international humanitarian law to instances of cyber attacks either in times of cyber warfare, real kinetic warfare or in peacetime, attribution of wrongful acts committed by non-state actors to States and detection and investigation of complex transborder cybercrimes are only a portion of the highly contentious issues that need to be addressed by Member States and which require a cautious approach on the part of the Rapporteur.

4. As regards "Progresses within AALCO", apart from closely pursuing the relevant developments concerning international law in cyberspace including those at the UN and CCPCJ on cybercrimes, the Islamic Republic of Iran has actively contributed to the relevant deliberations at AALCO at the meetings of the Open-ended Working Group on International Law in Cyberspace and during Annual Sessions as well. From the outset, we suggested that the work on the topic had better be focused on three main domains namely "State sovereignty in Cyberspace and internet governance", "cyber attacks" and "cybercrimes". As the work progressed and the Working Group deliberated the diverse relevant topics, the said items were covered and therefore it seemed there emerged a common understanding of the subject at hand. In this regard, the Special Study prepared by the Secretariat serves as a useful tool to catch up with the latest developments in the field. As the issues of concern have been raised during the Working Group sessions and also highlighted by the Secretariat and the Rapporteur alike, we support the proposal put forward by some Member States that the Rapporteur should develop AALCO guidelines or model provisions on Cyberspace. Due to the diverse aspects of the topic, however, we suggest that the scope of the work should be delineated to have a clear picture of the outcome. Further discussions during the sessions of the Working Group could be a useful indicator thereof.
5. As for "Suggestions as to the Future Plan of Action of the Working Group", we support the idea of continuing the discussions on the diverse topics named by the Rapporteur; notwithstanding modifications will be inevitable due to the ongoing deliberations by Member States and probably the latest developments of the topic in other initiatives and bodies.
6. On the basic framework and core elements of the AALCO guidelines or model provisions on Cyberspace, as part of the drafting process, first a few issues need to be cleared. Above all, as the topic under discussion has been from the scratch "International Law in Cyberspace", one expects that the Model in question needs to cover the diverse subtopics including sovereignty in cyberspace, peaceful use of cyberspace, international cooperation on combating cybercrime and the application and development of existing instruments. Whether to adopt a comprehensive approach – a painstaking and time-consuming effort -

or not, we agree that the topics may be determined before each meeting of the Working Group, with the aim of facilitating in-depth discussions; it remains clear, however, that the outline of the work needs to be set from the outset.

7. We highly support the idea of conducting researches on, and drawing up definitions for, such key terms as cyber attacks, cyber warfare, cyber terrorism, Internet governance and the like. Such an endeavor could, no doubt, build up on the bulwarks already set up by AALCO and could further pave the way for future contributions of Member States to the existing literature on international law in Cyberspace.
8. In the end, we thank the Special Rapporteur for his thorough research on the topic. The Islamic Republic of Iran continues to follow with interest the latest developments in international law in Cyberspace and is prepared to have further contributions to the relevant discussions at the Open-ended Working Group on International Law in Cyberspace.

**Comments of China to the *Report on the Future Plan of Action*
of the Working Group**

1. China highly appreciates the *Report on the Future Plan of Action of the Working Group* prepared by Prof. Zhixiong Huang, Rapporteur of the AALCO Working Group on International Law in Cyberspace. The Report represents in an objective and pragmatic manner a comprehensive description of overall development of international law in cyberspace and relevant work done within the framework of AALCO, as well as some practical proposals for enhancing AALCO Member States' cooperation in fighting cybercrime, deepening and broadening discussion on items of the Working Group, and strengthening information sharing, legal research and capacity building, etc., and therefore conducive to future work of the Working Group. China suggests that the Working Group convene its 3rd meeting before or during 2018 AALCO Annual Session to, among others, develop a work plan based on the Report, with a view to advancing its substantive work in a timely fashion.

2. The idea to develop model provisions on fighting cybercrime put forward in the Report is in line with practice of AALCO and common interests of its Member States, and is beneficial for strengthening AALCO's role in cyberspace global governance. China is in support of this idea. In addition, China would like to suggest that the main elements of the model provisions should include criminalization, jurisdiction, investigation and

prosecution, international cooperation, electronic evidence, crime prevention, technical assistance and capacity building, etc. We also suggest the Working Group to invite Member States to submit their inputs on framework and core elements of the Model Provisions before 2019 AALCO Annual Session; and based on the submissions, the Rapporteur, with assistance of the Secretariat, may prepare a set of Draft Model Provisions for consideration and adoption by Member States in the 2020 AALCO Annual Session. The Model Provisions are not legally binding, but could serve as a useful reference for Member States to strengthen national legislation, participate in international negotiation and formulate relevant international instruments, etc.

3. In addition, China suggests that AALCO may consider the adoption of a “Declaration on Principles of International Law in Cyberspace”, which would summarize and identify core common positions and values of AALCO Member States in application and development of international law in cyberspace. The declaration will voice our collective positions to the international community and enhance the influence of AALCO and its Member States as a whole in this realm. Elements of the declaration may include the following: respect state sovereignty in cyberspace, including sovereignty and jurisdiction over cyber infrastructures, data and activities in the territory of a state; promote a culture of establishing a common future for cyberspace, and adhere to the principle of extensive consultation, joint contribution and shared benefit, to build a multilateral, democratic and transparent global Internet governance system; adhere to non-use of force and peaceful resolution of disputes in cyberspace, and prevent militarization of and arms race in cyberspace; promote international cooperation in cyberspace, jointly prevent and combat criminal and terrorist use of cyberspace, etc.

Annexure 4

Japan's comments on draft "Report on the Future Plan of Action of the Working Group Meeting"

Japan appreciates the efforts of Prof. Zhixiong Huang, Rapporteur of the AALCO Working Group on International Law in Cyberspace. The draft report presents a concise picture of the discussion on international law in cyberspace at various international forums and also recaptures different views expressed thus far by Member States of AALCO.

1. Our comment concerns the suggestions for the future plan of action of the Working Group, in particular, the proposal for development of prospective AALCO guidelines or model provisions on cyberspace (page 10, "A. Enhancing AALCO Member States' cooperation in countering cybercrime"). The entire section is presented in favor of this particular action by drawing on the views expressed by some, not all, Member States during past Annual Sessions, the proposal made by the Rapporteur at the 2nd meeting of the Working Group, and the conclusion of the Special Study on International Law in Cyberspace.

While Japan is aware that some Member States are supportive of developing a new global legal instrument pertaining to cybercrime and that these views have been expressed by some Member States at past Annual Sessions and Working Group meetings, there has been no consensus on this particular position, nor on other positions for that matter, among Member States. Neither did the Summary Report of the 2nd meeting of the Working Group or the Special Study obtain endorsement of Member States. Rather, they *took note* of these outcomes (AALCO/RES/56/S17, PP4 and PP5).

Japan regards that it would be premature to draft a specific plan of action based solely on one side of the argument and to forego other positions. More discussion would be needed among Member States before drawing a particular proposal on an issue that entails different views/positions. Japan would like to point out that, pursuant to United Nations General Assembly resolution 65/230, practical discussion to counter cybercrime, including the discussion on whether new instruments such as model provisions are necessary in the field of countering cybercrime, is already under way at the Open-ended

Intergovernmental Expert Group Meeting on Cybercrime (IEG) of CCPCJ, where Asia and African countries' representatives also participate and that AALCO should avoid duplicating this ongoing work.

Therefore, Japan proposes that paragraphs 14-16 be removed from the draft report and an alternative suggestion such as follows be included:

“Member States are encouraged to continue discussion on possible cooperation in countering cybercrime to complement the ongoing efforts in other international forums such as CCPCJ.”

2. In addition, as for “Conducting research on terminology” (para.18), Japan regards that it is necessary to first agree on which terms in particular need to be studied. And if the purpose is to promote common understanding among AALCO Member States, the necessity of publication should be reconsidered.

Therefore, Japan proposes that paragraph 18 be modified as follows:

“In order to promote common understanding among AALCO Member States on the key issues of international law in cyberspace, it is helpful for Member States, with support of the Secretariat and the Rapporteur of the Working Group, to conduct research on the key terms agreed by the Member States.”

3. The above comments and other points are reflected in the attached draft report.

END

**Asian-African Legal Consultative Organization
Working Group on International Law in Cyberspace**

Report on the Future Plan of Action of the Working Group

Zhixiong Huang*, Rapporteur of the
AALCO Working Group on International Law in Cyberspace

1. The Asian-African Legal Consultative Organization (hereinafter referred to as “AALCO”) adopted Resolution AALCO/RES/56/S 17 at its Fifty-Sixth Annual Session on 5 May 2017 which, among others, “directs the Rapporteur of the Open-ended Working Group on International Law in Cyberspace (hereinafter referred to as “the Working Group”) to prepare a Report on the basis of the discussions that have taken place thus far among the Member States, and the Special Study prepared by the Secretariat, laying down a future plan of action for the Working Group.” This Report, drafted pursuant to that mandate, is divided into three parts: (I) Development of International Law in Cyberspace; (II) Progresses within AALCO so far; (III) Suggestions as to the Future Plan of Action of the Working Group.

I. Development of International Law in Cyberspace

2. It has been generally agreed that the sui generis character of cyberspace does not preclude it from regulation of existing rules and principles of international law, and that the fundamental tenet of international law, i.e. state sovereignty is intrinsically linked with internet governance.¹ In the meantime, there is also a consensus that “[g]iven the unique attributes of ICTs, additional norms could be

* Luo Jia Chair Professor and Vice Dean, Law School of Wuhan University, China.

¹ International Law in Cyberspace, AALCO/54/BEIJING/2015, para.4.

developed over time”.² Currently, a number of international institutions and processes have touched on the issues related to the development and application of international rules, among which, the following two platforms within the framework of the United Nations are particularly noteworthy.

3. Consisting of representatives from the 5 permanent members of the United Nations Security Council and other 10-20 States, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter referred to as “GGE”) has been regarded as one of the most influential inter-governmental mechanisms exploring possible consensus on application and development of international rules for cyberspace. In June 2013, a consensual final report adopted by the 3rd GGE (2012-2013) confirmed that “[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment”.³ In June 2015, the 4th GGE (2014-2015) adopted a new consensual final report, which proposed 11 paragraphs on voluntary, non-binding norms, rules or principles of responsible behavior of States, as well as 6 paragraphs on how international law applies to the use of ICTs by States.⁴ However, due mainly to controversies over specific issues regarding the application of certain rules of international law (e.g. the right to self-defense, international humanitarian law, and state responsibility) to cyberspace, the 5th GGE (2016-2017) comprised of 25 States failed to reach a new final report.⁵

4. In the area of combating cybercrime, the UN General Assembly, in its resolution 65/230 in 2010, requested the Commission on Crime Prevention and Criminal Justice (hereinafter referred to as “CCPCJ”) to establish an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of

² See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para. 16; United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 15.

³ See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para.11, paras. 19-20.

⁴ See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 13, para. 28.

⁵ See UNODA, Developments in the Field of Information and Telecommunications in the Context of International Security, <https://www.un.org/disarmament/topics/informationsecurity>.

cybercrime and responses to it by Member States, the international community and the private sector, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime (hereinafter referred to as “IEG”).⁶ The first session of the IEG was held in Vienna from 17 to 21 January 2011. At that session, the IEG reviewed and adopted a collection of topics and a methodology for the study. In its resolution 67/189, the General Assembly noted with appreciation the work of the IEG and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the CCPCJ in due course. The second session of the IEG was held from 25 to 28 February 2013. At that session, the IEG, *inter alia*, took note of the *draft comprehensive study of the problem of cybercrime*⁷ and responses to it by Member States, the international community and the private sector, as prepared by the United Nations Office on Drugs and Crime (UNODC) under the auspices of the IEG, pursuant to the mandate contained in General Assembly resolution 65/230. This draft study offered several options to strengthen existing and to propose new national and international legal or other responses to cybercrime, including the development of international model provisions; development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters; development of a comprehensive multilateral instrument on cybercrime; and delivery of enhanced technical assistance for the prevention and combating of cybercrime in developing countries. The third session of the IEG took place in Vienna from 10 to 13 April 2017. Based on the recommendations of the third session, the CCPCJ in its resolution 26/4 requests the IEG to continue its work and, in so doing, to hold periodic meetings and function as the platform for further discussion on substantive issues concerning cybercrime.⁸

⁶ <http://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html>

⁷ The methodology for the study tasked the United Nations Office on Drugs and Crime with developing the study, including developing a questionnaire for the purposes of information gathering, collecting and analyzing data, and developing a draft text of the study. Information gathering in accordance with the methodology, including the distribution of a questionnaire to Member States, intergovernmental organizations and representatives from the private sector and academic institutions, was conducted by UNODC, from February 2012 to July 2012. Information was received from 69 Member States with regional distribution as follows: Africa (11), Americas (13), Asia (19), Europe (24), and Oceania (2). Information was received from 40 private sector organizations, 16 academic organizations and 11 intergovernmental organizations. Over 500 open source documents were also reviewed by the Secretariat. This draft study offered several options to strengthen existing and to propose new national and international legal or other responses to cybercrime, including the development of international model provisions; development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters; development of a comprehensive multilateral instrument on cybercrime; and delivery of enhanced technical assistance for the prevention and combating of cybercrime in developing countries.

⁸ Report on the meeting of the Open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 10 to 13 April 2017, UNODC/CCPCJ/EG.4/2017/4; The Commission on Crime Prevention and Criminal Justice, Strengthening international cooperation to combat cybercrime, Resolution

Pursuant to the above CCPCJ resolution and aims to facilitate its implementation, the Chair of IEG proposed the 2018–2021 work plan⁹ of the IEG recently and will be adopted at the forthcoming 4th IEG meeting to be held in 3-5 April 2018. It is expected that the IEG will be a main forum for international rules-making on combating cybercrime in the coming years.

5. It is also noteworthy that Russian Federation recently submitted a *Draft United Nations Convention on Cooperation in Combating Information Crimes* to the United Nations General Assembly as an UN official document (A/C.3/72/12). It is the first suggestion on a global Convention on cybercrime to the UNGA by a state.

II. Progresses within the Framework of AALCO so far

6. Based on the recommendation of the People's Republic of China, Member States of AALCO agreed to incorporate the topic "International Law in Cyberspace" as a regular agenda item at the Fifty-third Annual Session in Tehran, Iran in September 2014.¹⁰ This agenda item was also deliberated in the Fifty-fourth Annual Session held in Beijing, China in April 2015, during which the Member States decided to establish an Open-ended Working Group on International Law in Cyberspace to further discuss the matter through meetings or workshops to be cosponsored with Governments of the Member States or relevant international organizations.¹¹

7. In the First Meeting of AALCO Working Group on International Law in Cyberspace convened in New Delhi during the Fifty-Fifth Annual Session of AALCO on 19 May 2016, H.E. Mr. Hossein Panahi Azar, then Director General for International Legal Affairs, Ministry of Foreign Affairs, Islamic Republic of Iran, H.E. Ms. Njeri Mwangi Wachira, Chief State Counsel, Kenya, and Prof. Zhixiong Huang of Wuhan University Law School of the People's Republic of China, were

26/4,
http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCCPJ_Res_Dec/CCPCJ-R-ES-26-4.pdf

⁹ Main topics for 2018-2020 meetings including: Legislation & frameworks; Criminalization; Law enforcement & investigations; Electronic evidence & criminal justice; International cooperation; Prevention. No later than 2021, the IEG will hold stock-taking meeting that will finish consideration of all the preliminary conclusions and recommendations and will produce a consolidated list of adopted conclusions and recommendations for submission to the CCPCJ.

<http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/V1800915.pdf>.

¹⁰ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/53/S17, 18 SEPTEMBER 2014.

¹¹ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/DFT/54/S17, 17 APRIL 2015.

respectively elected as the Chairperson, Vice-Chairperson and Rapporteur of the Working Group. During the meeting, delegates addressed some important issues such as applicability of international law in cyberspace, the domestic legal framework, State sovereignty in cyberspace, rules of international cooperation in combating cybercrimes, and future work of the Working Group. A resolution adopted at that Annual Session encourages Member States to actively participate in relevant regional and global fora deliberating on the governance of cyberspace and to strengthen their communication and cooperation in this regard; directs the Working Group to hold inter-sessional meetings, preferably in cooperation with Member States and relevant international organizations and other institutions, in pursuance of its mandate; and also directs the Secretariat to closely follow the developments in international forums related to governance of cyberspace and cyber security.¹²

8. During 9-10 February 2017, the second meeting of the Open-ended Working Group on International Law in Cyberspace was convened at AALCO Headquarters in New Delhi. 23 Member States of AALCO participated in the meeting.¹³ Six sessions were held during the 2-day meeting. The inaugural session comprised of addresses by the Secretary General of AALCO Prof. Kennedy Gastorn, the President of the Fifty-Fifth Annual Session of AALCO Dr. V.D. Sharma, and the Chairperson of the Working Group Mr. Hossein Panahi Azar on the present day importance of the topic, “International Law in Cyberspace” and the continued relevance of the Working Group respectively. The next four sessions dealt with four major areas: State sovereignty in cyberspace, law and governance of cyberspace, cyber warfare, and cybercrimes and international law. Three experts Mr. Arun Mohan Sukumar, Head, Cyber Initiative, Observer Research Foundation, Mr. Jeremy England, Head of ICRC in New Delhi and Dr. Zhixiong Huang, Professor, Wuhan University Law School of the People’s Republic of China, and the Rapporteur of the Working Group, as guest speakers, gave their introductory speeches on sovereignty in cyberspace, cyber warfare and cybercrimes respectively, Member States presented their statements and had interactions with the experts. In the concluding session, the Secretariat briefly

¹² RESOLUTION ON “INTERNATIONAL LAW IN CYBERSPACE”, AALCO/RES/DFT/55/S17, 20 MAY 2016.

¹³ Arab Republic of Egypt, People’s Republic of China, Cyprus, Democratic People’s Republic of Korea, India, Indonesia, Islamic Republic of Iran, Japan, Malaysia, Mongolia, Myanmar, Nepal, Sultanate of Oman, State of Qatar, Kingdom of Saudi Arabia, South Africa, Sri Lanka, State of Palestine, Tanzania, Sudan, Syrian Arab Republic, Thailand and Republic of Yemen. See, Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.137

introduced the content of its Special Study on international law in cyberspace which will be released in the coming Annual Session of AALCO. Member States also had the opportunity to discuss the future work of the Working Group, the suggestion of having a Model Law in place as regards rules of international law in combating cybercrimes was proposed.¹⁴

9. On 5 May 2017, the topic of international law in cyberspace was discussed by AALCO Member States during the Fifty-Sixth Annual Session held in Nairobi, Kenya, preceded by a Summary Report of the Chairperson of the Open-ended Working Group on International Law in Cyberspace, on the 2nd Working Group Meeting. Several issues, of which the state sovereignty and fundamental human rights in cyberspace, Internet governance, international cooperation in combating cybercrime, law of armed conflict and state responsibility in cyberspace, etc, were discussed. Member States recognized the imperative role of AALCO in promoting Member States to share insights and reach consensus on the issues mentioned above.¹⁵ The resolution adopted during the Annual Session, inter alia, directed the Rapporteur of the Open-ended Working Group on International Law in Cyberspace to prepare a Report on the basis of the discussions that have taken place thus far among the Member States, and the Special Study prepared by the Secretariat, laying down a future plan of action for the Working Group.¹⁶

10. Thus far, discussions among AALCO Member States have focused on the following topics: international law pertaining to State Sovereignty in cyberspace, peaceful use of cyberspace, rules of international cooperation in combating cybercrimes, identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace and law and governance of Cyberspace, etc.¹⁷ On international law pertaining to State Sovereignty in cyberspace, while many countries, by invoking the consensus reached by the GGE,¹⁸ reaffirmed the

¹⁴ Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, pp.137-139.

¹⁵ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.143, p.145.

¹⁶ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/DFT/56/S17, 5 MAY 2017.

¹⁷ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/DFT/54/S17, 17 APRIL 2015.

¹⁸ United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para. 20; United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 27.

application of the principle of State Sovereignty in cyberspace, they also concerned with the questions such as the exercise of extra-territorial criminal jurisdiction,¹⁹ data based jurisdiction,²⁰ and the need to strike a proper balance between sovereign rights in cyberspace and the protection of fundamental human rights, such as freedom of expression and confidentiality of communication.²¹ On the peaceful use of cyberspace, Member States mainly concerned about the escalation in militarization of the cyberspace,²² and clarification of the standards for legal attribution of cyber activities to a state.²³ Some Member States pointed out that under some circumstances, cyber activities could amount to the use of force or an armed attack within the context of UN Charter and customary international law.²⁴ While others cautioned that many elements pertaining to this issue remain open to discussion, and stressed that no abuse may be tolerated in resort to force or self-defense, and the sanctity of article 2(4) of the UN Charter must remain intact in all circumstances.²⁵ On the rules of international cooperation in combating cybercrimes, some Member States underscored the importance of the Convention on Cybercrime of the Council of Europe (or the Budapest Convention), emphasized that appropriate consideration should be given so as not to duplicate the efforts by creating something very similar to the Budapest Convention.²⁶ Some other Members criticized the Budapest Convention as being fundamentally unbalanced and questioned its legitimacy and long-effectiveness.²⁷ The need to have a multilateral treaty that would effectively prevents escalation of cybercrime, preferably through a UN-centric governance model

¹⁹ See, e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.166.

²⁰ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.144.

²¹ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.188; Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.165.

²² See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.81.

²³ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.145.

²⁴ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.151.

²⁵ See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, pp.166-167; Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.151 and p.148.

²⁶ See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, pp.165.

²⁷ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.187 and Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.167.

for cyberspace, was clearly supported by some Member States.²⁸ On the identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace, some Member States stated that the unique characteristics of network technology necessitate a renewed debate and considered international effort to develop the criteria that would determine the application of international law and principles to cyberspace, since the current legal framework is not enough to provide solutions to the security dilemma posed by cyberspace security attacks.²⁹ Other Members also pointed to the fact that cyberspace remains a domain which lacks of substantial rules and regulations due to its intangibility, and highlighted the need to step up our efforts to develop and promote the norms, rules and principles to be applied to cyberspace.³⁰ On the law and governance of cyberspace, Member States introduced and reviewed latest progresses made in their domestic cyber policies, legislation and institution development. While some in support of a multi-stakeholder approach that neither the government nor the industry has the monopolistic dominance over one another,³¹ others in support of a multilateral management of the Internet whereby United Nations serves as the main channel in promoting the adoption of accepted international rules in cyberspace, and all states would have a share in the regulation and management of the Internet.³² Some even called on AALCO to adopt of its resolution to prepare an international convention for the regulation of cyberspace in order to ensure the use of cyberspace for the service of mankind.³³

11. AALCO Secretariat, pursuant to the relevant mandate by Member States, has been closely following developments in international forums related to governance of cyberspace and cyber security. Besides the Open-ended Working Group meetings organized by the Secretariat mentioned above, it also organized, with the financial and logistical support from the Government of People's Republic of China, a side event on

²⁸ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.181.

²⁹ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.88 and p.190.

³⁰ Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.143.

³¹ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.145.

³² See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.162 and Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/Nairobi/2017/VR, p.141.

³³ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.193.

the theme “Enhancing International Cooperation on Combating Cybercrimes” during the 25th session of CCPCJ on 23 May 2016 at the UN Office in Vienna, Austria.³⁴ On the invitation from the Chinese Ministry of Foreign Affairs to AALCO, the Secretary-General of AALCO attended the 4th World Internet Conference (WIC) held at Wuzhen International Internet Exhibition and Convention Center in Wuzhen, China from 3-5 December, 2017. The Secretary-General presented a paper on “Relevance of International Law in Combating Cybercrime: Current Issues and AALCO’s Approach” at the session on “International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes”. Moreover, mandated by the resolution adopted at the Fifty-Fourth Annual Session, AALCO Secretariat prepared a Special Study on International Law in Cyberspace,³⁵ which was released during the Fifth-Sixth Annual Session held in Nairobi, Kenya in May 2017.

12. In short, AALCO Member States have stressed the significance of the principles and rules of international law applicable to cyberspace, including ~~those in~~ the UN Charter, and ~~the need for further study of, and deliberation on, discussion and development of~~ rules of international law on cyberspace issues~~[, and exploring the areas of further development of international law on the issue as appropriate]~~.³⁶ In particular, the importance of international cooperation in combating cybercrime has been frequently stressed in previous discussions in AALCO. For example, the resolution adopted by AALCO Member States mandated the Working Group “to hold inter-sessional meetings, preferably in cooperation with Member States and relevant international organizations and other institutions in particular the United Nations in pursuance of its mandate, *taking into account the need of AALCO Member States in combating cybercrime*” (emphasis added).³⁷ It also underlined the need for enhanced coordination and judicial cooperation among Member States in combating the criminal misuse of information and communication technologies.³⁸

Commented [情報通信課1]: We propose the same language as in the resolution adopted, i.e. AALCO/RES/56/S17.

III. Suggestions as to the Future Plan of Action of the Working Group

³⁴ AALCO’s Side Event “Enhancing International Cooperation on Combating Cybercrimes” was Held in Vienna, <http://www.aalco.int/Side%20Event.pdf>

³⁵ AALCO Secretariat, International Law in Cyberspace, New Delhi, 2017.

³⁶ See, e.g., RESOLUTION ON “INTERNATIONAL LAW IN CYBERSPACE”, AALCO/RES/~~DFT~~56/S17, 5 MAY 2017.

³⁷ RESOLUTION ON “INTERNATIONAL LAW IN CYBERSPACE”, AALCO/RES/DFT/55/S17, 20 MAY 2016.

³⁸ Id.

13. The unique attributes of cyberspace have raised a number of important legal challenges relating to the application of international law in cyberspace.³⁹ On the basis of the discussions that have taken place thus far among the Member States and studies conducted by the Secretariat, the following suggestions are offered for consideration of a future plan of action of the Working Group.

~~A. Enhancing AALCO Member States' cooperation in countering cybercrime~~

~~14. Cybercrime is now a global threat. According to the Global Risks Report 2016, global cost of cybercrime will reach \$ 2 trillion by 2019, a threefold increase from the 2015 estimate of \$ 500 billion.⁴⁰ Because of the transnational nature of cybercrime, international cooperation in extradition, mutual legal assistance, mutual recognition of foreign judgments, and police to police cooperation, are essential. Yet, a prominent feature of international cooperation in this area is fragmentation at the international level, and diversity of national cybercrime laws.⁴¹ In order to effectively combat cybercrime, the existing instruments and mechanisms must be harmonized and improved. This is why some Member States who are already Contracting Parties to one or several existing instruments stressed the need for a global comprehensive instrument pertaining to cybercrime.⁴² As such, some delegations called upon AALCO Secretariat to conduct a detailed study on the appropriate rules of international cooperation in combating cybercrime which may thereafter lead to the formation of a guideline in this aspect.⁴³ Besides, the Chairperson's Summary Report of the 2nd Meeting of Open ended Working Group on International Law in Cyberspace proposed that, the future work priority and outcome of the Working Group could be the prospective AALCO guidelines or model provisions on cyberspace.⁴⁴ One of the important concrete conclusions in the Special Study on~~

³⁹ See e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/Nairobi/2017/VR, p.144.

⁴⁰ See *Global Risks Report 2016*, <http://reports.weforum.org/global-risks-2016/>

⁴¹ Currently there are several regional initiatives in combating cybercrime, including the 2001 Convention on Cybercrime of the Council of Europe (also known as the Budapest Convention), the 2010 League of Arab States Convention on Combating Information Technology Offenses, the 2001 Commonwealth of Independent States Agreement on Cooperation in Combating Offenses related to Computer Information, the 2010 Shanghai Cooperation Organization Agreement in the Field of International Information Security, and the African Union Convention on Cybersecurity and Personal Data Protection.

⁴² See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.98.

⁴³ See Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.167.

⁴⁴ Chairperson's Summary Report of the 2nd Meeting of Open ended Working Group on International Law in Cyberspace, <http://www.aalco.int/Working%20Group%20Report%202017.pdf>.

International Law in Cyberspace prepared by AALCO Secretariat is that it is important for nations to come together to work on uniform rules of international law for curbing cyber crimes.⁴⁵ It also follows with the last sentence of the Study states: “It has brought out the glaring defect that till now cyber crimes have been regulated haphazardly and in piecemeal fashion, with there being national legislations, and many binding as well as non-binding regional and international instruments regulating cybercrimes, with overlapping or even sometimes conflicting provisions.”

15. In past decades, AALCO Member States already gained extensive experience in drafting principles or model articles on issues such as extradition of fugitive offenders,⁴⁶ admission and treatment of aliens,⁴⁷ elimination or reduction of dual or multiple nationality,⁴⁸ and promotion and protection of investment.⁴⁹ These principles and draft articles have played an important role in deepening discussions and forging consensus among AALCO Member States.

16. From the above, it may be fair to say that drafting a set of model provisions on preventing and combating cybercrime within the framework of AALCO could serve as a useful first step for the future work of the Working Group. The drafting process may operate in the following steps: first, all Member States of AALCO will be invited to submit written comments on the basic framework and core elements of the Model Provisions. Second, with the assistance of AALCO Secretariat, the Rapporteur of the Working Group may be mandated to prepare, based on the written submissions of the Member States of AALCO, a Draft Model Provisions for the consideration of Working Group. Third, the Working Group will be mandated to formulate, based on the Draft of the Rapporteur, a Model Provisions to be adopted by AALCO Annual Session.

BA. Deepening discussions on some key issues of international law in cyberspace among AALCO Member States

⁴⁵ AALCO Secretariat, *International Law in Cyberspace*, New Delhi, 2017, pp.112-113.

⁴⁶ ARTICLES CONTAINING THE PRINCIPLES CONCERNING EXTRADITION OF FUGITIVE OFFENDERS, <http://www.aalco.int/ARTICLES%20CONTAINING%20THE%20PRINCIPLES%20CONCERNING%20EXTRA-DITION%20OF%20FUGITIVE%20OFFENDERS.pdf>.

⁴⁷ PRINCIPLES CONCERNING ADMISSION AND TREATMENT OF ALIENS, <http://www.aalco.int/PRINCIPLES%20CONCERNING%20ADMISSION%20AND%20TREATMENT%20OF%20ALIENS.pdf>.

⁴⁸ MODEL ARTICLES EMBODYING PRINCIPLES RELATING TO ELIMINATION OR REDUCTION OF DUAL OR MULTIPLE NATIONALITY, <http://www.aalco.int/Model%20Articles%20Embodying%20Principles.pdf>.

⁴⁹ PROMOTION AND PROTECTION OF INVESTMENTS, <http://www.aalco.int/PROMOTION%20AND%20PROTECTION%20OF%20INVESTMENTS.pdf>.

Enhancing AALCO Member States' cooperation in countering cybercrime

Cybercrime is now a global threat. According to the Global Risks Report 2016, global cost of cybercrime will reach \$ 2 trillion by 2019, a threefold increase from the 2015 estimate of \$ 500 billion.⁵⁰ Because of the transnational nature of cybercrime, international cooperation in extradition, mutual legal assistance, mutual recognition of foreign judgments, and police-to-police cooperation, are essential. Given this background, Member States are encouraged to continue discussion on possible cooperation in countering cybercrime to complement the ongoing efforts in other international forums such as GGE and CCPCJ.

Commented [情報通信課2]: Taken from original paragraph 14.

17. Setting up crosscutting sub-topics. Four topics, i.e. sovereignty in cyberspace, peaceful use of cyberspace, international cooperation on combating cybercrime and the application and development of existing instruments, have been included in the agenda items of the Working Group. In order to facilitate further discussions among AALCO Member States on these topics, sub-topics on crosscutting issues such as sovereignty on data ~~and equal participation in international governance of the Internet~~ under the topic of sovereignty in cyberspace, or digital evidence and trans-boundary data collecting under the topic of international cooperation on combating cybercrime may be set up. They can be designated before each meeting of the Working Group, with the aim of facilitating in-depth discussions.

Commented [情報通信課3]: Given the existing multi-stakeholder forums on Internet governance and the lack of expertise for AALCO legal experts in relation to Internet policies and technologies, Japan questions as to whether AALCO is an appropriate forum to discuss Internet governance.

18. Conducting research on terminology. In order to promote common understandings among AALCO Member States on the key issues of international law in cyberspace, it's helpful for the Member States, with the support of the Secretariat and the Rapporteur of the Working Group, to conduct research on the key terms agreed by the Member States, ~~on such key terms as hacker attack, cyber warfare, cybercrime, cyber terrorism, governance of cyberspace (or Internet governance), Internet surveillance, critical cyber infrastructure, etc. In the end, a list of terms can be published.~~⁵¹

19. Adding new topics where appropriate. In accordance with the new

⁵⁰ See *Global Risks Report 2016*, <http://reports.weforum.org/global-risks-2016/>

⁵¹ It's noteworthy that in view of the importance of such terms, the International Telecommunication Union (ITU), The Internet Corporation for Assigned Names and Numbers (ICANN), the National Institute of Standards and Technology (NIST) of the United States have already published (and periodically updated) definitions of cyber-related terms. The NATO think tank CCD COE also compiles and researches the terms relating to cyber-security. See, e.g. Glossary of ICANN, <https://www.icann.org/resources/pages/glossary-2014-02-03-en>; Glossary of Key Information Security Terms, NIST, <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>; Cyber-Definitions of NATO Cooperative Cyber Defence Center of Excellency, <https://ccedcoe.org/cyber-definitions.html>.

development in international law in cyberspace and the practical needs of AALCO Member States, new topics beyond those four existing topics such as international rules on digital economy may be added to the agenda items.

EB. Strengthening capacity building in AALCO

20. Information-gathering and research by the Secretariat. The Secretariat may engage in further information gathering and research on all existing and future topics of the Working Group, so as to provide useful support to the discussion of those topics by the Working Group.

21. Establishing platforms for information-sharing. With the support and involvement of AALCO Member States, the Secretariat may upload relevant legislations and policy documents of the Member States and new achievements relating to international legislations to the official website of AALCO, which could be an invaluable platform for information-sharing among the Member States.

22. Carrying out international exchange and cooperation program. Close cooperation on concrete program between AALCO Member States and the Secretariat should be encouraged and further explored through joint effort by the Secretariat and Member States. One latest example is an international seminar on combating cybercrime held by the Chinese government in cooperation with AALCO during the 3rd Training Session of the China-AALCO Exchange and Research Program in International Law in September 2017. Organization of similar events should be encouraged in the future.

Annexure 5

Asian-African Legal Consultative Organization Working Group on International Law in Cyberspace

Report on the Future Plan of Action of the Working Group

Zhixiong Huang*, Rapporteur of the
AALCO Working Group on International Law in Cyberspace

1. The Asian-African Legal Consultative Organization (hereinafter referred to as “AALCO”) adopted Resolution AALCO/RES/56/S 17 at its Fifty-Sixth Annual Session on 5 May 2017 which, among others, “directs the Rapporteur of the Open-ended Working Group on International Law in Cyberspace (hereinafter referred to as “the Working Group”) to prepare a Report on the basis of the discussions that have taken place thus far among the Member States, and the Special Study prepared by the Secretariat, laying down a future plan of action for the Working Group.” This Report, drafted pursuant to that mandate, is divided into three parts: (I) Development of International Law in Cyberspace; (II) Progresses within AALCO so far; (III) Suggestions as to the Future Plan of Action of the Working Group.

I. Development of International Law in Cyberspace

2. It has been generally agreed that the sui generis character of cyberspace does not preclude it from regulation of existing rules and principles of international law, and that the fundamental tenet of international law, i.e. state sovereignty is intrinsically linked with internet governance.¹ However, it is noteworthy that some international law concepts which appear to be crystal clear in other areas still remain

* LuoJia Chair Professor and Vice Dean, Law School of Wuhan University, China.

¹ International Law in Cyberspace, AALCO/54/BEIJING/2015, para.4.

in the gray zone of international law when it comes to cyberspace and there's little consensus on their exact definition and application at the international level. In the meantime, there is also a consensus that "[g]iven the unique attributes of ICTs, additional norms could be developed over time".² The intricacies and complexities of the cyberspace still require further regulation at the international level, which is to be developed based on the existing principles of international law and to which, AALCO could make important contributions. Currently, a number of international institutions and processes have touched on the issues related to the development and application of international rules, among which, the following two platforms within the framework of the United Nations are particularly noteworthy.

3. Consisting of representatives from the 5 permanent members of the United Nations Security Council and other 10-20 States, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter referred to as "GGE") has been regarded as one of the most influential inter-governmental mechanisms exploring possible consensus on application and development of international rules for cyberspace. In June 2013, a consensual final report adopted by the 3rd GGE (2012-2013) confirmed that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".³ In June 2015, the 4th GGE (2014-2015) adopted a new consensual final report, which proposed 11 paragraphs on voluntary, non-binding norms, rules or principles of responsible behavior of States, as well as 6 paragraphs on how international law applies to the use of ICTs by States.⁴ However, due mainly to controversies over specific issues regarding the application of certain rules of international law (e.g. the right to self-defense, international humanitarian law, and state responsibility) to cyberspace, the 5th GGE (2016-2017) comprised of 25 States failed to reach a new

² See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para. 16; United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 15.

³ See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para. 11, paras. 19-20.

⁴ See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 13, para. 28.

final report.⁵

4. In the area of combating cybercrime, the UN General Assembly, in its resolution 65/230 in 2010, requested the Commission on Crime Prevention and Criminal Justice (hereinafter referred to as “CCPCJ”) to establish an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime (hereinafter referred to as “IEG”).⁶ The first session of the IEG was held in Vienna from 17 to 21 January 2011. At that session, the IEG reviewed and adopted a collection of topics and a methodology for the study. In its resolution 67/189, the General Assembly noted with appreciation the work of the IEG and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the CCPCJ in due course. The second session of the IEG was held from 25 to 28 February 2013. At that session, the IEG, inter alia, took note of the *draft comprehensive study of the problem of cybercrime*⁷ and responses to it by Member States, the international community and the private sector, as prepared by the United Nations Office on Drugs and Crime (UNODC) under the auspices of the IEG, pursuant to the mandate contained in General Assembly resolution 65/230. This draft study offered several options to strengthen existing and to propose new national and international legal or other responses to cybercrime, including the development of international model provisions; development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters; development of a comprehensive multilateral instrument on cybercrime; and delivery of enhanced technical assistance

⁵ See UNODA, Developments in the Field of Information and Telecommunications in the Context of International Security, <https://www.un.org/disarmament/topics/informationsecurity>.

⁶ <http://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html>

⁷ The methodology for the study tasked the United Nations Office on Drugs and Crime with developing the study, including developing a questionnaire for the purposes of information gathering, collecting and analyzing data, and developing a draft text of the study. Information gathering in accordance with the methodology, including the distribution of a questionnaire to Member States, intergovernmental organizations and representatives from the private sector and academic institutions, was conducted by UNODC, from February 2012 to July 2012. Information was received from 69 Member States with regional distribution as follows: Africa (11), Americas (13), Asia (19), Europe (24), and Oceania (2). Information was received from 40 private sector organizations, 16 academic organizations and 11 intergovernmental organizations. Over 500 open source documents were also reviewed by the Secretariat. This draft study offered several options to strengthen existing and to propose new national and international legal or other responses to cybercrime, including the development of international model provisions; development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters; development of a comprehensive multilateral instrument on cybercrime; and delivery of enhanced technical assistance for the prevention and combating of cybercrime in developing countries.

for the prevention and combating of cybercrime in developing countries. The third session of the IEG took place in Vienna from 10 to 13 April 2017. Based on the recommendations of the third session, the CCPCJ in its resolution 26/4 requests the IEG to continue its work and, in so doing, to hold periodic meetings and function as the platform for further discussion on substantive issues concerning cybercrime.⁸ Pursuant to the above CCPCJ resolution and aims to facilitate its implementation, the Chair of IEG proposed the 2018–2021 work plan⁹ of the IEG recently and will be adopted at the forthcoming 4th IEG meeting to be held in 3-5 April 2018. It is expected that the IEG will be a main forum for international rules-making on combating cybercrime in the coming years.

5. It is also noteworthy that Russian Federation recently submitted a *Draft United Nations Convention on Cooperation in Combating Information Crimes* to the United Nations General Assembly as an UN official document (A/C.3/72/12). It is the first suggestion on a global Convention on cybercrime to the UNGA by a state.

II. Progresses within the Framework of AALCO so far

6. Based on the recommendation of the People's Republic of China, Member States of AALCO agreed to incorporate the topic "International Law in Cyberspace" as a regular agenda item at the Fifty-third Annual Session in Tehran, Iran in September 2014.¹⁰ This agenda item was also deliberated in the Fifty-fourth Annual Session held in Beijing, China in April 2015, during which the Member States decided to establish an Open-ended Working Group on International Law in Cyberspace to further discuss the matter through meetings or workshops to be cosponsored with Governments of the Member States or relevant international organizations.¹¹

⁸ Report on the meeting of the Open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 10 to 13 April 2017, UNODC/CCPCJ/EG.4/2017/4; The Commission on Crime Prevention and Criminal Justice, Strengthening international cooperation to combat cybercrime, Resolution 26/4,

http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCPCJ_Res_Dec/CCPCJ-RES-26-4.pdf

⁹ Main topics for 2018-2020 meetings including: Legislation & frameworks; Criminalization; Law enforcement & investigations; Electronic evidence & criminal justice; International cooperation; Prevention. No later than 2021, the IEG will hold stock-taking meeting that will finish consideration of all the preliminary conclusions and recommendations and will produce a consolidated list of adopted conclusions and recommendations for submission to the CCPCJ,

<http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/V1800915.pdf>.

¹⁰ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/53/S17, 18 SEPTEMBER 2014.

¹¹ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/ 54/SP2, 17 APRIL 2015.

7. In the First Meeting of AALCO Working Group on International Law in Cyberspace convened in New Delhi during the Fifty-Fifth Annual Session of AALCO on 19 May 2016, H.E. Mr. Hossein Panahi Azar, then Director General for International Legal Affairs, Ministry of Foreign Affairs, Islamic Republic of Iran, H.E. Ms. Njeri Mwangi Wachira, Chief State Counsel, Kenya, and Prof. Zhixiong Huang of Wuhan University Law School of the People's Republic of China, were respectively elected as the Chairperson, Vice-Chairperson and Rapporteur of the Working Group. During the meeting, delegates addressed some important issues such as applicability of international law in cyberspace, the domestic legal framework, State sovereignty in cyberspace, rules of international cooperation in combating cybercrimes, and future work of the Working Group. A resolution adopted at that Annual Session encourages Member States to actively participate in relevant regional and global fora deliberating on the governance of cyberspace and to strengthen their communication and cooperation in this regard; directs the Working Group to hold inter-sessional meetings, preferably in cooperation with Member States and relevant international organizations and other institutions, in pursuance of its mandate; and also directs the Secretariat to closely follow the developments in international forums related to governance of cyberspace and cyber security.¹²

8. During 9-10 February 2017, the second meeting of the Open-ended Working Group on International Law in Cyberspace was convened at AALCO Headquarters in New Delhi. 23 Member States of AALCO participated in the meeting.¹³ Six sessions were held during the 2-day meeting. The inaugural session comprised of addresses by the Secretary General of AALCO Prof. Kennedy Gastorn, the President of the Fifty-Fifth Annual Session of AALCO Dr. V.D. Sharma, and the Chairperson of the Working Group Mr. Hossein Panahi Azar on the present day importance of the topic, "International Law in Cyberspace" and the continued relevance of the Working Group respectively. The next four sessions dealt with four major areas: State sovereignty in cyberspace, law and governance of cyberspace, cyber warfare, and cybercrimes and international law. Three experts Mr. Arun Mohan Sukumar, Head, Cyber Initiative,

¹² RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/DFT/55/S17, 20 MAY 2016.

¹³ Arab Republic of Egypt, People's Republic of China, Cyprus, Democratic People's Republic of Korea, India, Indonesia, Islamic Republic of Iran, Japan, Malaysia, Mongolia, Myanmar, Nepal, Sultanate of Oman, State of Qatar, Kingdom of Saudi Arabia, South Africa, Sri Lanka, State of Palestine, Tanzania, Sudan, Syrian Arab Republic, Thailand and Republic of Yemen. See, Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.137

Observer Research Foundation, Mr. Jeremy England, Head of ICRC in New Delhi and Dr. Zhixiong Huang, Professor, Wuhan University Law School of the People's Republic of China, and the Rapporteur of the Working Group, as guest speakers, gave their introductory speeches on sovereignty in cyberspace, cyber warfare and cybercrimes respectively, Member States presented their statements and had interactions with the experts. In the concluding session, the Secretariat briefly introduced the content of its Special Study on international law in cyberspace which will be released in the coming Annual Session of AALCO. Member States also had the opportunity to discuss the future work of the Working Group, the suggestion of having a Model Law in place as regards rules of international law in combating cybercrimes was proposed.¹⁴

9. On 5 May 2017, the topic of international law in cyberspace was discussed by AALCO Member States during the Fifty-Sixth Annual Session held in Nairobi, Kenya, preceded by a Summary Report of the Chairperson of the Open-ended Working Group on International Law in Cyberspace, on the 2nd Working Group Meeting. Several issues, of which the state sovereignty and fundamental human rights in cyberspace, Internet governance, international cooperation in combating cybercrime, law of armed conflict and state responsibility in cyberspace, etc., were discussed. Member States recognized the imperative role of AALCO in promoting Member States to share insights and reach consensus on the issues mentioned above.¹⁵ The resolution adopted during the Annual Session, inter alia, directed the Rapporteur of the Open-ended Working Group on International Law in Cyberspace to prepare a Report on the basis of the discussions that have taken place thus far among the Member States, and the Special Study prepared by the Secretariat, laying down a future plan of action for the Working Group.¹⁶

10. Thus far, discussions among AALCO Member States have focused on the following topics: international law pertaining to State Sovereignty in cyberspace, peaceful use of cyberspace, rules of international cooperation in combating cybercrimes, identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace and law and governance of Cyberspace,

¹⁴ Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, pp.137-139.

¹⁵ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.143, p.145.

¹⁶ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/DFT/56/S17, 5 MAY 2017.

etc.¹⁷ On international law pertaining to State Sovereignty in cyberspace, while many countries, by invoking the consensus reached by the GGE,¹⁸ reaffirmed the application of the principle of State Sovereignty in cyberspace, they also concerned with the questions such as the exercise of extra-territorial criminal jurisdiction,¹⁹ data based jurisdiction,²⁰ and the need to strike a proper balance between sovereign rights in cyberspace and the protection of fundamental human rights, such as freedom of expression and confidentiality of communication.²¹ On the peaceful use of cyberspace, Member States mainly concerned about the escalation in militarization of the cyberspace,²² and clarification of the standards for legal attribution of cyber activities to a state.²³ Some Member States pointed out that under some circumstances, cyber activities could amount to the use of force or an armed attack within the context of UN Charter and customary international law.²⁴ While others cautioned that many elements pertaining to this issue remain open to discussion, and stressed that no abuse may be tolerated in resort to force or self-defense, and the sanctity of article 2(4) of the UN Charter must remain intact in all circumstances.²⁵ On the rules of international cooperation in combating cybercrimes, some Member States underscored the importance of the Convention on Cybercrime of the Council of Europe (or the Budapest Convention), emphasized that appropriate consideration should be given so as not to duplicate the efforts by creating something very similar to the Budapest Convention.²⁶ Some other Members criticized the Budapest Convention

¹⁷ RESOLUTION ON “INTERNATIONAL LAW IN CYBERSPACE”, AALCO/RES/ 54/SP2, 17 APRIL 2015.

¹⁸ United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), Sixty-eighth session, A/68/98, para. 20; United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), Seventieth session, A/70/170, para. 27.

¹⁹ See, e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.166.

²⁰ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.144.

²¹ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.188; Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.165.

²² See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.81.

²³ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.145.

²⁴ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.151.

²⁵ See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, pp.166-167; Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.151 and p.148.

²⁶ See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, pp.165.

as being fundamentally unbalanced and questioned its legitimacy and long-effectiveness.²⁷ The need to have a multilateral treaty that would effectively prevents escalation of cybercrime, preferably through a UN-centric governance model for cyberspace, was clearly supported by some Member States.²⁸ On the identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace, some Member States stated that the unique characteristics of network technology necessitate a renewed debate and considered international effort to develop the criteria that would determine the application of international law and principles to cyberspace, since the current legal framework is not enough to provide solutions to the security dilemma posed by cyberspace security attacks.²⁹ Other Members also pointed to the fact that cyberspace remains a domain which lacks of substantial rules and regulations due to its intangibility, and highlighted the need to step up our efforts to develop and promote the norms, rules and principles to be applied to cyberspace.³⁰ On the law and governance of cyberspace, Member States introduced and reviewed latest progresses made in their domestic cyber policies, legislation and institution development. While some in support of a multi-stakeholder approach that neither the government nor the industry has the monopolistic dominance over one another,³¹ others in support of a multilateral management of the Internet whereby United Nations serves as the main channel in promoting the adoption of accepted international rules in cyberspace, and all states would have a share in the regulation and management of the Internet.³² Some even called on AALCO to adopt of its resolution to prepare an international convention for the regulation of cyberspace in order to ensure the use of cyberspace for the service of mankind.³³

11. AALCO Secretariat, pursuant to the relevant mandate by Member States, has

²⁷ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.187 and Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.167.

²⁸ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.181.

²⁹ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.88 and p.190.

³⁰ Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.143.

³¹ See, e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/NAIROBI/2017/VR, p.145.

³² See e.g. Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.162 and Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/Nairobi/2017/VR, p.141.

³³ See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.193.

been closely following developments in international forums related to governance of cyberspace and cyber security. Besides the Open-ended Working Group meetings organized by the Secretariat mentioned above, it also organized, with the financial and logistical support from the Government of People's Republic of China, a side event on the theme "Enhancing International Cooperation on Combating Cybercrimes" during the 25th session of CCPCJ on 23 May 2016 at the UN Office in Vienna, Austria.³⁴ On the invitation from the Chinese Ministry of Foreign Affairs to AALCO, the Secretary-General of AALCO attended the 4th World Internet Conference (WIC) held at Wuzhen International Internet Exhibition and Convention Center in Wuzhen, China from 3-5 December, 2017. The Secretary-General presented a paper on "Relevance of International Law in Combating Cybercrime: Current Issues and AALCO's Approach" at the session on "International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes". Moreover, mandated by the resolution adopted at the Fifty-Fourth Annual Session, AALCO Secretariat prepared a Special Study on International Law in Cyberspace,³⁵ which was released during the Fifth-Sixth Annual Session held in Nairobi, Kenya in May 2017.

12. In short, AALCO Member States have stressed the significance of the principles and rules of international law applicable to cyberspace, including those in the UN Charter, and the need for further study of, deliberation on, rules of international law on cyberspace issues, and to explore the areas of further development of international law on the issue as appropriate.³⁶ In particular, the importance of international cooperation in combating cybercrime has been frequently stressed in previous discussions in AALCO. For example, the resolution adopted by AALCO Member States mandated the Working Group "to hold inter-sessional meetings, preferably in cooperation with Member States and relevant international organizations and other institutions in particular the United Nations in pursuance of its mandate, *taking into account the need of AALCO Member States in combating cybercrime*" (emphasis added).³⁷ It also underlined the need for enhanced coordination and judicial cooperation among Member States in combating the

³⁴ AALCO's Side Event "Enhancing International Cooperation on Combating Cybercrimes" was Held in Vienna, <http://www.aalco.int/Side%20Event.pdf>

³⁵ AALCO Secretariat, *International Law in Cyberspace*, New Delhi, 2017.

³⁶ See, e.g., RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/ 56/S17, 5 MAY 2017.

³⁷ RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE", AALCO/RES/ 55/S17, 20 MAY 2016.

criminal misuse of information and communication technologies.³⁸

III. Suggestions as to the Future Plan of Action of the Working Group

13. The unique attributes of cyberspace have raised a number of important legal challenges relating to the application of international law in cyberspace.³⁹ On the basis of the discussions that have taken place thus far among the Member States and studies conducted by the Secretariat, the following suggestions are offered for consideration of a future plan of action of the Working Group.

A. Enhancing AALCO Member States' cooperation in countering cybercrime

14. Cybercrime is now a global threat. According to the Global Risks Report 2016, global cost of cybercrime will reach \$ 2 trillion by 2019, a threefold increase from the 2015 estimate of \$ 500 billion.⁴⁰ Because of the transnational nature of cybercrime, international cooperation in extradition, mutual legal assistance, mutual recognition of foreign judgments, and police-to-police cooperation, are essential. Yet, a prominent feature of international cooperation in this area is fragmentation at the international level, and diversity of national cybercrime laws.⁴¹ In order to effectively combat cybercrime, the existing instruments and mechanisms must be harmonized and improved. This is why some Member States who are already Contracting Parties to one or several existing instruments stressed the need for a global comprehensive instrument pertaining to cybercrime.⁴² As such, some delegations called upon AALCO Secretariat to conduct a detailed study on the appropriate rules of international cooperation in combating cybercrime which may thereafter lead to the formation of a guideline in this aspect.⁴³ Besides, the Chairperson's Summary Report of the 2nd Meeting of Open-ended Working Group on International Law in

³⁸ Id.

³⁹ See e.g. Verbatim Record of Discussions during Fifty-Sixth Annual Session, AALCO/56/Nairobi/2017/VR, p.144.

⁴⁰ See *Global Risks Report 2016*, <http://reports.weforum.org/global-risks-2016/>

⁴¹ Currently there are several regional initiatives in combating cybercrime, including the 2001 Convention on Cybercrime of the Council of Europe (also known as the Budapest Convention), the 2010 League of Arab States Convention on Combating Information Technology Offenses, the 2001 Commonwealth of Independent States Agreement on Cooperation in Combating Offenses related to Computer Information, the 2010 Shanghai Cooperation Organization Agreement in the Field of International Information Security, and the African Union Convention on Cybersecurity and Personal Data Protection.

⁴² See, e.g. Verbatim Record of Discussions during Fifty-Fourth Annual Session, AALCO/54/BEIJING/2015/VR, p.98.

⁴³ See Verbatim Record of Discussions during Fifty-Fifth Annual Session, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, p.167.

Cyberspace proposed that, the future work priority and outcome of the Working Group could be the prospective AALCO guidelines or model provisions on cyberspace.⁴⁴ One of the important concrete conclusions in the Special Study on International Law in Cyberspace prepared by AALCO Secretariat is that it is important for nations to come together to work on uniform rules of international law for curbing cyber-crimes.⁴⁵ It also follows with the last sentence of the Study states: “It has brought out the glaring defect that till now cyber-crimes have been regulated haphazardly and in piecemeal fashion, with there being national legislations, and many binding as well as non-binding regional and international instruments regulating cybercrimes, with overlapping or even sometimes conflicting provisions.”

15. In past decades, AALCO Member States already gained extensive experience in drafting principles or model articles on issues such as extradition of fugitive offenders,⁴⁶ admission and treatment of aliens,⁴⁷ elimination or reduction of dual or multiple nationality,⁴⁸ and promotion and protection of investment.⁴⁹ These principles and draft articles have played an important role in deepening discussions and forging consensus among AALCO Member States.

16. Given this background, Member States are encouraged to continue discussion on possible cooperation in countering cybercrime, including adopting 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 such as CCPCJ.⁵⁰ For that purpose, inputs from all Member States of AALCO as to the basic framework and core elements of the Model Provisions are to be welcomed.

B. Deepening discussions on some key issues of international law in

⁴⁴ Chairperson’s Summary Report of the 2nd Meeting of Open-ended Working Group on International Law in Cyberspace, <http://www.aalco.int/Working%20Group%20Report%202017.pdf>.

⁴⁵ AALCO Secretariat, International Law in Cyberspace, New Delhi, 2017, pp.112-113.

⁴⁶ ARTICLES CONTAINING THE PRINCIPLES CONCERNING EXTRADITION OF FUGITIVE OFFENDERS, <http://www.aalco.int/ARTICLES%20CONTAINING%20THE%20PRINCIPLES%20CONCERNING%20EXTRA%20DITION%20OF%20FUGITIVE%20OFFENDERS.pdf>.

⁴⁷ PRINCIPLES CONCERNING ADMISSION AND TREATMENT OF ALIENS, <http://www.aalco.int/PRINCIPLES%20CONCERNING%20ADMISSION%20AND%20TREATMENT%20OF%20ALIENS.pdf>

⁴⁸ MODEL ARTICLES EMBODYING PRINCIPLES RELATING TO ELIMINATION OR REDUCTION OF DUAL OR MULTIPLE NATIONALITY, <http://www.aalco.int/Model%20Articles%20Embodying%20Principles.pdf>.

⁴⁹ PROMOTION AND PROTECTION OF INVESTMENTS, <http://www.aalco.int/PROMOTION%20AND%20PROTECTION%20OF%20INVESTMENTS.pdf>.

⁵⁰ The Rapporteur modified this paragraph according to Japan’s Comments on draft “Report on the Future Plan of Action of the Working Group Meeting”.

cyberspace among AALCO Member States

17. Setting up crosscutting sub-topics. Four topics, i.e. sovereignty in cyberspace, peaceful use of cyberspace, international cooperation on combating cybercrime and the application and development of existing instruments, have been included in the agenda items of the Working Group. In order to facilitate further discussions among AALCO Member States on these topics, sub-topics on crosscutting issues such as sovereignty on data and equal participation in international governance of the Internet under the topic of sovereignty in cyberspace, or digital evidence and trans-boundary data collecting under the topic of international cooperation on combating cybercrime may be set up. They can be designated before each meeting of the Working Group, with the aim of facilitating in-depth discussions.

18. Conducting research on terminology. In order to promote common understandings among AALCO Member States on the key issues of international law in cyberspace, it's helpful for the Member States, with the support of the Secretariat and the Rapporteur of the Working Group, to conduct research on such key terms as cyber attack, cyber warfare, cybercrime, cyber terrorism, governance of cyberspace (or Internet governance), Internet surveillance, critical cyber infrastructure, etc, to be agreed by Member States. In the end, a list of terms can be published.⁵¹

19. Adding new topics where appropriate. In accordance with the new development in international law in cyberspace and the practical needs of AALCO Member States, new topics beyond those four existing topics such as international rules on digital economy may be added to the agenda items.

C. Strengthening capacity building in AALCO

20. Information-gathering and research by the Secretariat. The Secretariat may engage in further information gathering and research on all existing and future topics of the Working Group, so as to provide useful support to the discussion of those topics by the Working Group.

21. Establishing platforms for information-sharing. With the support and

⁵¹ It's noteworthy that in view of the importance of such terms, the International Telecommunication Union (ITU), The Internet Corporation for Assigned Names and Numbers (ICANN), the National Institute of Standards and Technology (NIST) of the United States have already published (and periodically updated) definitions of cyber-related terms. The NATO think tank CCD COE also compiles and researches the terms relating to cyber security. See, e.g. Glossary of ICANN, <https://www.icann.org/resources/pages/glossary-2014-02-03-en>; Glossary of Key Information Security Terms, NIST, <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>; Cyber Definitions of NATO Cooperative Cyber Defence Center of Excellency, <https://ccdcoe.org/cyber-definitions.html>.

involvement of AALCO Member States, the Secretariat may upload relevant legislations and policy documents of the Member States and new achievements relating to international legislations to the official website of AALCO, which could be an invaluable platform for information-sharing among the Member States.

22. Carrying out international exchange and cooperation program. Close cooperation on concrete program between AALCO Member States and the Secretariat should be encouraged and further explored through joint effort by the Secretariat and Member States. One latest example is an international seminar on combating cybercrime held by the Chinese government in cooperation with AALCO during the 3rd Training Session of the China-AALCO Exchange and Research Program in International Law in September 2017. Organization of similar events should be encouraged in the future.

D. Adopting a Declaration on Principles of International Law in Cyberspace.

23. AALCO may consider the adoption of a “Declaration on Principles of International Law in Cyberspace”, which would summarize and identify core common positions and values of AALCO Member States in application and development of international law in cyberspace. The declaration will voice Member States’ collective positions to the international community and enhance the influence of AALCO and its Member States as a whole in this realm. Elements of the declaration may include the following: respect state sovereignty in cyberspace, including sovereignty and jurisdiction over cyber infrastructures, data and activities in the territory of a state; promote a culture of establishing a common future for cyberspace, and adhere to the principle of extensive consultation, joint contribution and shared benefit, to build a multilateral, democratic and transparent global Internet governance system; adhere to non-use of force and peaceful resolution of disputes in cyberspace, and prevent militarization of and arms race in cyberspace; promote international cooperation in cyberspace, jointly prevent and combat criminal and terrorist use of cyberspace, etc.



Annexure 6

Asian African Legal
Consultative Organization

4 SEP 2018

File No. 95 (1)

Time 11.30 AM

HIGH COMMISSION FOR PAKISTAN
NEW DELHI

No.Pol-9/20/2018

August 30, 2018

The High Commission for the Islamic Republic of Pakistan presents its compliments to the Asian-African Legal Consultative Organization in New Delhi and has the honour to refer to AALCO's note verbale No.176/2018/WGM/AALCO dated 6 August 2018 regarding "Report on the Future Plan of Action of the Working Group Meeting" prepared by Prof. Zhixiong Huang, Special Rapporteur of the AALCO Working Group on the International Law in Cyberspace".

The Mission has the honour to enclose herewith comments received from concerned department in Pakistan on the above-mentioned report.

The High Commission for the Islamic Republic of Pakistan avails itself of this opportunity to renew to the Asian-African Legal Consultative Organization the assurances of its highest consideration.

Encl: As above.

The Asian-African Legal
Consultative Organization (AALCO) Secretariat,
29-C, Rizal Marg, Diplomatic Enclave,
Chanakyapuri, New Delhi-110021



pg. 50

2/50-G, Shantipath, Chanakyapuri, New Delhi - 110021

Phones : (91-11) 26110601/2/5. Fax : (91-11) 26872339.

E-mail : pahicnewdelhi@mofa.gov.pk,

E-mail : pakhcnd@gmail.com

Website : www.pakhcnewdelhi.org.pk

Website : www.mofa.gov.pk/newdelhi

**Comments on "Report on the Future Plan of Action of the
Working Group Meeting"**

The subject report has been examined in concerned department in Pakistan. This report is divided into three parts which are as follows.

- a) Development of International Law in Cyberspace.
 - b) Progress within the Framework of AALCO so far.
 - c) Suggestion as to the Future Plan of Action of the Working Group.
-
- i. Pakistan has to provide no comments regarding first part at this point of time.
 - ii. In relation to progress within the framework of AALCO, it is important to point out that AALCO member states have focused on vital and sensitive issues of cyberspace which includes state sovereignty, peaceful use of cybercrime and rules of international cooperation in combating cybercrimes. These efforts are highly appreciated by this Division. Moreover it is suggested that AALCO should adopt work plan of Intergovernmental Expert Group Meeting on Cybercrime (IEG) in its coming sessions and also adopt efforts of IEG regarding electronic evidence in criminal matters.
 - iii. As regards the future plan of action, it is suggested that a web portal among the AALCO member states to be created for providing solution and guidance regarding cyber crime on reciprocal basis. Further it is suggested that AALCO should enter into an arrangement among its member states by which legal assistance regarding cyber crimes can be provided to one state by the other.