ASIAN-AFRICAN LEGAL CONSULTATIVE ORGANIZATION

SUMMARY REPORT OF THE FOURTH MEETING OF THE OPEN-ENDED WORKING GROUP ON INTERNATIONAL LAW IN CYBERSPACE

2-4 SEPTEMBER 2019

HANGZHOU, CHINA

---

1. Introduction

10 Member States of the Asian-African Legal Consultative Organization (AALCO) participated in the Fourth Meeting of the Open-ended Working Group on International Law in Cyberspace, namely **People's Republic of China, Islamic Republic of Iran, Republic of Iraq, Japan, Pakistan, State of Qatar, Kingdom of Saudi Arabia, Kingdom of Thailand, United Arab Emirates (UAE) and the Socialist Republic of Vietnam**. Representatives of **the International Committee of the Red Cross (ICRC)** were also present **as observer**.

The Members of the Bureau of the Open-ended Working Group who participated in the Meeting are as follows: (1) **Chairman: H.E. Dr. Abbas Bagherpour Ardekani**, Director-General for International Legal Affairs, Ministry of Foreign Affair, Islamic Republic of Iran and (2) **Rapporteur: Dr. Huang Zhixiong, Professor**, Wuhan University, People's Republic of China.

2. Welcoming Reception hosted by Zhejiang Provincial Department of Foreign Affairs

On 1 September 2019, a Welcoming Reception was hosted by Zhejiang Provincial Department of Foreign Affairs. A warm welcome to the historic and cultural city of Hangzhou was extended to all the delegates by **Mr. Yao Guowen, Deputy Director-General, Zhejiang Provincial Department of Foreign Affairs** and **Counsellor Mr. Wu Haiwen, Treaty and Law Department of the Ministry of Foreign Affairs of China**. Hangzhou is also a hub for information technology and is well-suited to host the Working Group Meeting on International Law in Cyberspace. The hosting of this Working Group Meeting is a reflection of China's commitment and continued endeavours in promoting cooperation on international law in cyberspace. **Secretary-General of AALCO, H.E. Prof. Dr. Kennedy Gastorn** and **the Chairman of the Working Group,** elucidated the objective behind the conception of AALCO and emphasized that the Open-ended Working Group on International Law in Cyberspace has been a platform to facilitate the interaction between Member States for the progressive development of international law on the topic. Appreciation was expressed to the Province of Zhejiang and the Ministry of Foreign Affairs of China for hosting the Working Group Meeting.

3. Inaugural Session

The Secretary-General, AALCO in his opening remarks spoke briefly on the establishment of the Open-ended Working Group and its work on international law in cyberspace since its inception including the deliberations involving the Member States. Mention was made of Meetings of the Open-Ended Working Group held so far, and the mandate of the Annual Session held in 2017 pursuant to which the Rapporteur was asked to prepare a Report on the Future Plan of Action of the Working Group, that was sent to all Member States for their comments and observations. He invited Member States to actively participate in the deliberations, which would facilitate the Working Group Meeting to decide the future plan of action of the Working Group and deliberations on the topic international law in cyberspace.

The Chairman in his opening remarks highlighted the pertinence of the topic international law in cyberspace, with the opportunities promised and the challenges posed. It was recalled that during the last three Working Group Meetings, the delegates deliberated upon crucial aspects of the topic, including State sovereignty in cyberspace, applicability of international law in cyberspace, State practice and cooperation for combating cybercrimes and future work of the Working Group. He thanked the Ministry of Foreign Affairs of China for organizing the Fourth Working Group Meeting and the rigorous ground work that has gone into the process. He noted that as the preparatory work for the upcoming Report on the "Special Need of the Member States for International Cooperation against Cybercrime", a questionnaire, prepared by the Rapporteur, was circulated among the Member States, to which responses from 11 Member States have been received. The commitment of AALCO to the topic under the able leadership of Prof. Dr. Kennedy Gastorn was lauded.

4. Proceedings of the Working Group Meeting on Cyberspace

The Chairman thereafter introduced the provisional agenda and programme of work, as presented to the Member States. Finding no objection to the same, the agenda and organization of work was adopted.

Topic I: International Cooperation for Combating Cybercrime (issues relating to Member States' response to the questionnaire)

The Rapporteur presented his Report on the outcome of the Member States' Response to the Questionnaire. The Rapporteur thanked the Chair for the opportunity to summarize the responses received from the Member States to the Questionnaire. By the end of June 2019, replies to the Questionnaire were received from 9 Member States. The responses of 2 States came only towards the end of August which could not be factored in the summary. All the replies received provide a useful source for understanding the special need of AALCO Member states for international cooperation against cybercrimes.

As regards domestic law on cybercrime, seven out of the 9 replying Member states confirmed that they had already formulated or amended their domestic laws on the subject. Most of them expressed similar views on the basic issues relating to the substantive law of cybercrime (conviction and sentencing). Most States had domestic laws involving criminal jurisdiction of cybercrime though these laws did not contain articles for coordinating criminal jurisdiction of cybercrime with other countries. Member States emphasized the importance of international coordination on this area.

The second part of the Questionnaire on international cooperation witnessed different attitudes of the replying Member States on most questions. The number of States which had joined the Budapest Convention on Cybercrime, the Agreement on Cooperation in Ensuring

International Information Security Between the Member States of the Shanghai Cooperation Organization and the League of Arab States was, respectively, one. Six States were not part of any Cybercrime Convention.

On the issue of capacity-building and technical assistance, all of them were of the view that they need a set of uniform standards for combating cybercrime and technical assistance in this regard. They also mentioned that most States had received technical assistance related to cybercrime and cyber security. On public-private partnership, it was agreed that cooperation from the private sector was useful in combating cybercrime.

Thereafter, the floor was given to two panelists to present on the first topic, i.e., international cooperation for combating cybercrime.

Mr. Dong Hanfei, Official from Ministry of Public Security, People's Republic of China adduced relevant current data to suggest that the Chinese netizens constitute 21% of internet users globally, and that 99% of those netizens use smart devices to access the internet. Of the major global internet market capitalization leaders, 7 out of 30 are from China, including Alibaba and Tencent.

It was pointed out that cyber security constitutes a non-traditional form of security, and the primary responsibilities of the Cyber Security Department of the Ministry of Public Security of China were enumerated. The four levels in the hierarchy of the institutional infrastructure in China to cater to cyber security are, namely, national- Cyber Security Department; provincial- Cyber Security Division; municipal- Cyber Security Detachment; and prefectural- Cyber Security Unit.

It was noted that commission of cybercrimes have undergone rapid increase in China, and most cases require specialized teams to address such conduct. The characteristics of cybercrimes, including cyber attributions to traditional crimes, independence from geo-location, and adoption of new technologies were discussed. The Chinese police countermeasures were noted. Suggestions were adduced to operationalize pragmatic cooperation via joint case investigation, technical assistance and training, information and intelligence sharing and conversations and dialogues; and the example of collaboration between Chinese law enforcement agencies and those from Thailand in 2013 to combat a cybercrime was cited.

Mr. Chen Liang, Deputy Director for Political Affairs, Tencent Group introduced Tencent as China's largest provider of integrated Internet services, and observed that the Internet could be seen as a system similar to a natural ecology, and cybercrimes could be perceived as parasites that live in the ecological system. It was noted that cybercrimes display certain characteristics and trends, including deep integration between cyberspace and offline society; industrialization of cybercrimes in the form of entire chains; commission of cybercrimes through more intelligent means; and cross-border nature of cybercrimes.

The steps taken by the Tencent Group in cooperating with the Chinese government to fight against cybercrimes were highlighted. The cases cited pertained to the abuse of AI to crack verification codes; blackmailing through DDoS attacks; and cross-border online blackmailing and fraud. The significance of the Tencent Guardians Project was accentuated in this context.

Thereafter, the Chairperson of the Working Group thanked the Rapporteur and the panelists and opened the floor for Member States for their general statements, comments, suggestions and views on the topic and seek any clarifications from the Rapporteur and panelists.

The ***delegate of Japan*** thanked the Chairman and the Rapporteur for his report. As a general comment it was mentioned that Japan realizes the importance of combating cybercrime and the need for cooperation on this front. It was stated that the Budapest Conventions was a useful framework for combating cybercrimes and a free and secure cyberspace was in the best interest of States.

The ***delegate of the Socialist Republic of Vietnam*** congratulated Prof. Huang and the other speakers. He highlighted the policies of Vietnam on Cyberspace and the domestic legislation of Vietnam dealing with Cybercrimes. The importance of AALCO Member States sharing their best practices in the area was encouraged as a good measure to facilitate international cooperation in this field. The delegate expressed his desire to receive the report of the Rapporteur and suggested the Rapporteur should expand his work beyond the responses received from the States and possibly adopt only after getting more State views. The delegate requested the first speaker to elaborate in greater detail on the four levels of combating cybercrimes existing in China and the policies pertaining to Bitcoins and cryptocurrencies. In addition, the challenges being faced by cloud computing and police to police cooperation with different countries for investigating cybercrimes by China was requested greater explanation. The delegate requested the second speaker to explain the foray of Tencent in Africa and partnership with law-enforcement officials.

The ***delegate of People's Republic of China***, welcomed all the delegates to the beautiful city of Hangzhou and thanked the Rapporteur and other two panelists for their presentations. It was pointed out that the report was a useful point of reference. He pointed out that the international community faces obstacles in tackling cybercrime due to fragmentation in international law in cyberspace. China continues to support the work of the UN on the subject. China has a strong framework for combating cybercrime. Challenges pertaining to data sovereignty were pointed out. He emphasized that AALCO Member States should follow the subject closely. He pointed out the limitations of the Budapest Convention and highlighted the need to evolve a new international law framework dealing with cybercrimes taking into account contemporary realities.

The ***delegate of the Islamic Republic of Iran*** expressed his gratitude to AALCO, the Government of China and the Province of Zhejiang for organizing and hosting the Fourth Working Group meeting. He pointed out that the Islamic Republic of Iran highly values the efforts of AALCO, in particular the Working Group, in bringing Members together on the significant topic of combating cybercrime and that the very participation of Member States on deliberations of the subject signifies the importance of the topic. The domestic and international efforts of the country in combating cybercrime such as cyber-specific laws and institutions including the Computer Crime Act of 2009, establishment of Cyber Police in 2011 and cooperation of relevant national authorities with foreign counterparts were highlighted in this regard. He also reiterated that lack of a sound and inclusive international legal instrument on combating cybercrime and the Unilateral Coercive Measures as international challenges have impaired international cooperation in the fight against cybercrime. The need for differentiating between cybercrime committed for material or other financial benefits with other crimes perpetrated for political purposes was highlighted. The Islamic republic of Iran considered the Working Group a convenient platform for Members to exchange ideas in a legal context and to contribute appropriate development of international law on cybercrime.

The ***delegate of the United Arab Emirates*** highlighted national and international efforts of the country on combating cybercrime. The country's strong domestic framework for combating cybercrime and elevating the country's cybersecurity was pointed out. Furthermore, the core focus areas of the national cybersecurity strategies of the UAE were briefly explained.

The panelists responded to the questions and comments made from the floor.

The Chair concluded the discussion by highlighting the importance of an appropriate framework specifically addressing the topic. Despite some divergent views, the need to collectively tackle the challenges remains the common concern of AALCO Member States. The need to find common ground between the States was the most important aspects of the topic and could form the basis of the next Annual Session of AALCO. The involvement of all countries in this process was important. With regard to the Rapporteur's ongoing work on cybercrime, the Chair suggested that he continue updating the Report pursuant to the responses of the Member States. AALCO may also proceed to seek, in a parallel manner, the guidance and assistance of the AALCO Secretariat under the leadership of the Secretary-General, to explore preparation of a non-paper and/or zero-draft reflecting the consensual basic principles of international law applicable in cyberspace. He would enable the delegates to reflect or comment on the proposal the following day.

Topic II: Challenging Issues of International Law in Cyberspace

1. Application of the Principle of Non-Interference in Cyberspace

Dr. Pavan Duggal, Advocate, Supreme Court of India and Chairman, International Commission on Cyber Security Law, presented that despite the absence of an international covenant on the topic and lack of common agreement on principles of cyber law at the global level, it is unambiguous that principles of international law do apply to cyberspace, as evinced by the practice of the ICRC and the Tallinn Manuals 1.0 and 2.0. The efforts at the international level to articulate legal norms pertaining to the topic, albeit partially, particularly the United Nations Governmental Group of Experts and the Convention on Cybercrime of the Council of Europe were noted, and the recent attempts by the States to formulate domestic cyber legislations and push for bilateral or regional initiatives to legalize cyber norms highlighted. The approaches of States like China, Russia, Vietnam, Belarus and Australia were enumerated and certain bilateral arrangements cited.

That the advent of new technologies like Artificial Intelligence, Internet of Things and Blockchain present new challenges on the applicability of the principle of non-interference in cyberspace was pointed out, and the need to define common minimum legal principles governing regulation of cyber security at the global level underlined. It was suggested that AALCO might constitute an internal committee to work on the crystallization and development of norms concerning applicability of principles of non-interference in cyberspace.

Prof. Huang Zhixiong, the Rapporteur of the Working Group, thereafter furnished an overview of the principle of non-interference. He stated that the prohibited act of interference consists of two elements, *viz.*, *domaine reserve* and coercion. Despite the vagueness of the key terms, the core meaning of what constitutes unlawful interference is reasonably clear and includes action aimed at States to do or abstain from doing something. The trend perceived in

the application of the principle before and after 2016 was analysed. Before 2016 the principle was mainly advocated by non-western States. A shift in the attitude occurred post 2016, primarily due to Russia's alleged interference in 2016 US Presidential election. Developing and developed States tend to promote the principle of non-interference due to different reasons. The interconnectivity in cyberspace and the "glass house dilemma" were referred to, and the possibility of striking "a North-South grand bargain" and the challenges explored.

Thereafter, the Chairperson thanked the panelists and opened the floor for Member States for their comments.

The ***delegate from People's Republic of China*** thanked the panelists for their presentations, He highlighted that the principle of non-intervention in cyberspace is a very significant one for international law. It is a crucial rule of customary international law and all States should follow this principle. Cyber intervention is a very serious issue and attempts to use cyber networks to create social unrest, sabotage critical infrastructure and instigating colour revolutions should be prohibited. Whether or not coercion is a requisite element for prohibited intervention remains unsettled from state practices. The specific circumstances of Cyberspace must be considered when applying the principle of non-intervention in this domain, as intervention in cyberspace is covert and has serious consequences. China has always followed the five principles of peaceful coexistence which includes the principle of non-intervention, this principle should be applied in cyberspace. When applying this principle to cyberspace, it is suggested that it be based on sovereign equality of nations, the respect to the development path selected by the State, adherence to the institutional safeguard as enshrined in the UN Charter and its purposes and principles. States should not employ the internet to interfere in the internal affairs of another country.

The ***delegate of the United Arab Emirates*** highlighted the importance of sovereignty and non-interference in the domain of cyberspace. He stated that the concept of "cyberspace" as a "common good" as highlighted in international law (in comparison to air, sea, land, and outer space) should be further considered. On the question of international norm building, the delegate pointed out that a "bottom up" approach should be considered, in comparison to only "top down" approaches imposing norms, notwithstanding any obligations on states subject to international law.

The ***delegate of Vietnam*** appreciated the presenters for their presentations. He stated that international law is applicable to cyberspace. Cyberspace is a new phenomenon, lessons should be taken from other domains like outer-space and law of the sea. He raised the issue as to whether the internet could be considered the "global heritage of mankind". He requested a clarification from Dr. Duggal regarding this aspect of "common heritage of mankind" and a clarification from Prof. Huang regarding the interface between fake news and the law of intervention.

The ***delegate of the Islamic Republic of Iran*** thanked the panelists for their presentations and appreciated the Working Group for its consideration of significant topics such as the application of non-intervention principle on cyberspace. He highlighted, from a general point of view, the importance of the principle of non-intervention as one of the fundamental principles on international law explaining its ambit and quoted the 1970Friendly Relations Declaration in this regard, which prohibits States or group of States from interfering in internal or external affairs of any other State. He pointed out that although the importance and general status of the principle of non-intervention is uncontested, the exact dimensions and contours of application of this principle on cyberspace is not clear, and that for this reason

the application of the principle of non-intervention should be taken into consideration. He also mentioned that for the present, given the general scope of the principle, the extraterritorial application of domestic laws by a State is a gross violation of the international law and constitutes an infringement of the principle of non-intervention, including, when the former aims to compel another State to alter its domestic laws and regulations related to internet. The Islamic Republic of Iran proposed the idea of an independent study and discussion of the topic by the Working Group in future works of AALCO.

The ***delegate of Japan*** thanked the Chair and the presenters. He highlighted that in general, when a State takes an action which denies the supreme authority of another State without its consent and lacking basis of international law, such an action constitutes infringement of territorial sovereignty. It is necessary to determine on a case by case basis about what sort of action in cyberspace constitutes infringement of territorial sovereignty. For the element of non-intervention to kick in, it is essential that the element of coercion is strongly made out, but it needs further study on how the principle of non-intervention is applied in cyberspace.

The ***delegate of ICRC*** pointed out the applicability of IHL in cyberspace and welcomed more discussions by States in this regard. She stated that asserting that IHL applies to cyber warfare should not be misunderstood as legitimizing cyber warfare. The limits imposed by IHL also govern and constrain any cyber operations to which States or other parties to an armed conflict might resort. IHL applies in addition to, and independently of, the requirements of the UN Charter.

After the panelists responded to the questions and comments, the Chair pointed out that principle of non-intervention is highly relevant in today's context. He highlighted the UN Charter and its provisions in this regard and stated the significance of this topic in the context of cyberspace. Further discussions were needed for the proper application of these principles in cyberspace.

Topic II: Challenging Issues of International Law in Cyberspace

2. Data Sovereignty, Transborder Data Flow and Data Security

Mr. Albert Liu, the Vice President & Deputy General Counsel of Alibaba Group, noted that different governance templates have been adopted, offered a perspective on data sovereignty, transborder data flow and data security assuming the goal of economic development and enablement, and walked the participants through the real life example of Alibaba's Electronic World Trading Platform, or eWTP initiative, to show how data regulation might impact such an empowering initiative. Acknowledging the complexities of data governance, the role of technology in creating a new digital economy was highlighted. Governments are increasingly challenged to understand and manage the new forms of digital, data-centric economies, which are increasingly cross border and increasingly drive cooperative interdependence between constituents in multiple jurisdictions, thereby challenging governments to figure out a framework that can both support such cross border collaboration while ensuring safety and security for its own citizens.

Technology and data, when harnessed in a benevolent manner, can be an inclusive equalizer for small and medium size businesses to reach the world. Certain key considerations for data regulation when the goal is digital economic development, which include cooperation among governments to set common standards, were enumerated.

Dr. Hong Yanqing, Research Director, International Development Research Institution, Peking University, PRC deliberated on the topic "Cross-border Data Flows in the trade negotiations: Implications for Data Sovereignty" pursuant to the ongoing negotiation under WTO framework on the digital economy chapter. The sub-topics under consideration were data localization and cross-border data flow, the nature of the concepts and stakes involved in the context. The extant arguments against cross-border data flow were cited. The existence of strict data localization policies despite the arguments against the same were noted and increasing adoption of measures regulating cross-border data flows was referred to. In order to decipher the emerging trends in trade negotiations, TPP benchmark was pitted against the language proposed by the US and the EU, with respect to ensuring the security and confidentiality of communications, cross-border transfer of information, protection of personal data and privacy, and the special category of cross-border transfer of financial data. The trend towards promoting data localization to ensure protection of individual as opposed to ensure data security appears to be the trend in the EU and the US.

Tracing the implications of this for data sovereignty, Chinese Cybersecurity Law's comprehensive definition of "data", and the WTO joint statement on e-commerce from Brazil with respect to measures to regulate cross-border data flow was referred to. Also, the rationale behind new concepts like "important data", whose breach, loss, abuse, etc. could harm the interests of the State and public interest, was explored. Questions were raised regarding the rights of countries to regulate cross-border data flow as they deem fit, and the role of WTO Negotiations to preserve State regulatory authority.

All the delegates who spoke thanked the panellists for their comprehensive and enlightening presentations.

The ***delegate of the United Arab Emirates*** highlighted the rights of states with regards to their sovereign rights to regulate their data and its security, including government, critical information infrastructure and personal data in its protection. In relation to international law, it was suggested that a point of focus should be to explore legal norms of extra-territoriality of states in relation to transborder data flow, in comparison to bilateral or multilateral agreements.

The ***delegate of People's Republic of China*** highlighted the position that transborder data flow poses a number of challenges to national security and privacy. There are differences in laws of various countries on trans border data flow and efforts to bridge the differences should be attempted. Security is the prerequisite for the free flow of data. States have the legitimate right to regulate the flow of data keeping in mind national security, public interest and privacy concerns. China, like other States has adopted measures to regulate data flow and the country will continue to adopt new measures keeping in mind emerging challenges. Exchange of best practices between States is important.

The ***delegate of Vietnam*** highlighted Vietnam's domestic position on the free flow of data. Appropriate provisions for data security exceptions are provided in the law including within the criminal law framework. The transnational flow of data has created numerous challenges for States, including need to protect citizens from terrorism and other forms of violence. Clarifications on the methodology of data classification and exception for Government data were requested.

The ***delegate of Islamic Republic of Iran*** stated that State sovereignty is one of the key principles of international law. Other key principles of international law also flow from the principle of State sovereignty. The domestic law of Iran to regulate data flow was elaborated.

The extra-territorial dimension of transborder data flow was highlighted and the need for foreign States to seek the consent of the host state to access data was emphasized. The delegate expressed interest in the future development of the topic.

The Panellists responed to the queries and clarifications of the delegations.

The Chair thanked the panelists and the delegates for their views. He emphasized the importance of this topic and highlighted the need for further discussions on this topic. The Chairman noted that further discussions would be required to define the concept of data security and to ensure that the principles of public international law, including that of state sovereignty, apply to this domain.

3. Regulating Online Harmful Content

Dr. Pavan Duggal stated that various kinds of harmful contents are available online, and in the absence of international regulation mechanisms, these are dealt with under national legislations. Examples were provided of the Malaysian Anti-Fake News Act of 2018 and other legislations based on the UNCITRAL Model Law on E-Commerce. Challenges that accrue as regards the scope of harmful contents, attribution, jurisdiction, role and responsibilities of intermediaries have led to a poor rate of cybercrimes conviction. The approaches of different States vary widely, and the practices of the US, India and New Zealand.

The relationship between cybercrimes and social media and the constant conflict between freedom of speech and expression and online harmful content was explored. Advent of new technologies like Artificial Intelligence, Internet of Things and Blockchain are further contributing to more online harmful content being generated. The need for international norms on this area was highlighted, and the initiatives taken so far by Russia, France and Germany in this regard were referred to.

The Chair thanked the panelist for the insightful presentation, and opened the floor for discussion.

The ***delegate of People's Republic of China*** observed that regulating online harmful content poses a global challenge, and dissemination of harmful content affects national security, public order and social stability. There is urgent need for the States to develop collective responses, and to define what constitutes harmful content. Certain elements of harmful content were enumerated from State practice. It was noted that China has been improving laws and regulations on this area, advocating for responsible behaviour in cyberspace. Respect for cyber sovereignty was emphasized, and the need to protect freedom of speech online without compromising national security underscored. The pertinence of international coordination and cooperation in strengthening administrative and law enforcement against such content was underlined.

The Chair accentuated the need to work together in discussing this issue deeply, and come to agreement with respect to what constitutes harmful content, and how it could be regulated for the protection of our societies, especially our children.

Topic III: Peaceful Use of Cyberspace

Ms. Margherita D'ascanio, Regional Legal Advisor and Head of Legal Department, ICRC East Asia highlighted the challenges posed by cyber operations on civilian population and civilian infrastructure during an armed conflict. It was pointed out that cyber operations

do not occur in a legal vacuum but are constrained by principles of international law, including international humanitarian law. The importance of detailed discussions on the interpretation of IHL for cyber operations was emphasized. All such discussions should be informed by an in-depth understanding of the development of military cyber capabilities, their potential human cost, and the protection already afforded by existing law. The panellist called upon all States to renew discussions in appropriate forums on the critical issues raised by cyberwarfare, with a view to finding common ground on the protection afforded by IHL to civilian use of cyberspace. The delegate offered ICRC's expertise on further discussions on this subject.

Dr. Du Yuejin, Vice Chairman of Cyber Security Association of China deliberated on cyber security crisis. Delving into the features of the coming new world, the panellist discussed in depth on the cyber war threat. The characteristics of such threat were enumerated, and that the current global mechanism to keep peace might be rendered useless noted. It does not fall within the ambit of war, in traditional sense of the term, with cyberweapons having three status: espionage, disruption and preparing for target. The unbalanced nature of such advanced and persistent threat which would proceed to launch targeted attacks was highlighted.

The purpose of studying cyberwarfare would be to try and stop it. The appropriate steps that could be taken were stated as: raising of awareness; trying to build, via concerted efforts, a new balanced global mechanism; and enhancing of capabilities, especially on discovering advanced cyber threat.

During the round of floor discussions, the ***delegate of Islamic Republic of Iran*** inquired as to the definition of cyber warfare.

The ***delegate of People's Republic of China*** emphasized on the need to raise awareness on cyberwar, and observed that inclusion of the same as a topic of discussion during the Working Group Meeting has been a welcome step towards that direction. As regards cyber attacks, debates exist on use of force and right of self-defense in the cyberspace. It was suggested that the UN Charter ought to apply as regards the prohibition on use of force and peaceful settlement of disputes. Cyber attacks could be launched by individuals and non-State actors as well, and it was inquired if dealing such attacks under the auspices of international criminal law would be appropriate.

It was submitted that although China supports discussion on international rules on cyber war, but deems the development of concrete rules premature owing to limited State practice. The regimes of *jus ad bellum* and *jus in bello* must apply taking note of the peculiarities of cyber warfare. Complexities also accrue as regards the applicability of the international humanitarian law principles of proportionality, distinction and neutrality. It was urged that the AALCO Member States ought to subscribe to peaceful use of cyberspace while keeping a close watch on development of rules on this area.

The ***delegate of Japan*** affirmed the applicability of Article 51 of the UN Charter to cyber warfare. As regards the threshold of use of force, the Law of War Manual published by the US Department of Defense was cited as a reference. It was suggested that disputes in cyberspace be resolved similar to the physical domain. Armed Conflict has not been defined in the Geneva Conventions, and ought to be defined on a case by case basis.

The Panellists responed to the queries and comments of the delegates.

The Chair concluded the session by noting that addressing the challenging and controversial issues of international law in cyberspace require further discussions within the traditional frameworks of *jus ad bellum* and *jus in bello*.

IV. Other Matters

As regards the way forward on the work of the Working Group, the Chairman set forth a two-fold proposal:

1. That the Member States ought to be more active in responding to the questionnaire of the Rapporteur, circulated in furtherance of preparation of the Report on the "Special Need of the Member States for International Cooperation against Cybercrime", as per the mandate received in the Fifty-seventh Annual Session of AALCO in Tokyo in 2018;
2. That the Member States seek the guidance and assistance of the Secretary-General to explore the drafting of a non-binding general document, a zero draft, clarifying the consensual basic principles of international law applicable in cyberspace.

The Chair invited the views of the delegates of the Member States on the second proposal.

Support was expressed by the ***delegate of the United Arab Emirates*** and ***Islamic Republic of Iran***. The ***delegate of People's Republic of China*** also expressed strong support, and encouraged the Member States to provide guidance and assistance to the Secretary-General and the Secretariat, as needed, in the preparation of the document.

Accordingly, the Chair's proposal was unanimously adopted.

V. Closing of the Meeting

The Draft Summary Report and the Draft Chairman's Report were circulated among the delegates of the Member States for their consideration and comments. In absence of any suggestions on modification, both the Reports were adopted.

Closing remarks were delivered by the Secretary-General and the Chairman. The Secretary-General in his concluding address expressed satisfaction over the successful culmination of the Fourth Working Group Meeting of International Law in Cyberspace. He highlighted the ever growing importance of the topic and China's strong support for AALCO and the need for international lawyers to keep abreast with rapidly emerging developments in the field. Secretary-General appreciated the role of the Rapporteur, Prof. Zhixiong Huang of the Wuhan University Law School for his meticulous and untiring work on the subject over the years. Member States who participated in the proceedings were acknowledged for their role in contributing to State practice in the subject. In addition, the Chairman was admired for the smooth and systematic conduct of the sessions. Before concluding, Secretary-General thanked, the provincial government of Zhejiang province and the Department of Treaty and Law, Ministry of Foreign Affairs, Government of China for hosting the Fourth Working Group Meeting and being excellent hosts. The efforts of Ms. Wang Liyu, Deputy-Secretary General and the legal team, AALCO was acknowledged as being instrumental to the success to the programme.

The Chairman in his final concluding remarks stated the way forward of the work of the Working Group. He suggested that the Member States seek the guidance and assistance of the Secretary-General to explore the drafting of a non-binding general document, a zero draft, clarifying the consensual basic principles of international law applicable in cyberspace, and

encouraged the Member States to provide guidance and assistance to the Secretary-General and the Secretariat, as needed, in the preparation of the document.

The Chairman expressed his gratitude on behalf of the meeting to the Rapporteur, the Secretary-General of AALCO and the AALCO Secretariat for their work on the topic in general. He also thanked all the panelists for their contribution in enriching the deliberation among the delegates of the Member States. He reiterated his gratitude to the host and all the participating delegations of the Member States.

The Fourth Meeting of the Open-ended Working Group on International Law in Cyberspace was thereafter adjourned.