AALCO/56/NAIROBI/2017/SD/S17
For official use only

ASIAN-AFRICAN LEGAL CONSULTATIVE ORGANIZATION

INTERNTIONAL LAW IN CYBERSPACE

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

INTERNATIONAL LAW IN CYBERSPACE

CONTENTS

INTERNATIONAL LAW IN CYBERSPACE

I. INTRODUCTION

A. Background

1. There has been a tremendous growth and expansion in the field of Information and Communication Technologies in the recent past. This evolution which is unprecedented in the field of technologies has not been complemented at par by the related developments in the concomitant laws and regulations in the international field. However, notwithstanding this lag, international law in cyberspace has, nevertheless, relatively speaking made significant advancements within a reasonably short period of time, in generating new norms over innovative platforms, for the regulation of various aspects of cyberspace.

2. Being aware 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. The topic has thereafter been discussed at all subsequent Annual Sessions of AALCO, with an open-ended Working Group having being formed at the Fifty-Fifth Annual Session with a mandate provided by the Fifty-Fourth Annual Session to study and deliberate upon a few flagged sub-topics within the broader topic as afore-stated. The Open-ended Working Group met once at the Fifty-Fifth Annual Session in 2016, and then as per the resolution adopted at the said session, at an inter-sessional meeting in February, 2017, at the AALCO Secretariat.

3. The sub-topics identified at the Fifty-Fourth Annual Session were, a) international law pertaining to State Sovereignty in cyberspace, b) peaceful use of cyberspace, c) rules of international cooperation in combating cybercrimes, and d) identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace. Furthermore, the resolution adopted at the Fifty-Fourth Annual Session mandated the AALCO Secretariat to prepare a Study on the topic "International Law in Cyberspace", as per the sub-topics identified in the Session, mentioned herein above. The Study will be released during the 2017 Annual Session.

4. The 2nd Open-ended Working Group Meeting on Cyberspace discussed four broad topics which had been derived from the discussions that had taken place between Member-States at the Annual Sessions of AALCO:

    1) State Sovereignty in Cyberspace: It was discussed between the Member States and the guest speaker that in spite of the global recognition that the principle of

sovereignty is applicable to cyberspace, as laid down at forums such as the UN World Summits on Information Society, and the UN Groups of Governmental Experts, States have widely experienced an erosion of sovereignty over it, which is a matter of great concern. Only a handful of countries are in a position to exercise jurisdiction over the important cyber-entities, as a result of which the rest of the States are finding it challenging to exercise sovereignty over incidents of cyber-attacks, cyber-crimes as well as over cyber-related businesses within their territories. Therefore, it is important that in addition to a general obligation on States to exercise their rights of sovereignty over cyberspace while respecting the rights of other States in this regard, it is also important that the international community comes up with legal norms to resolve this issue.

2) Law and Governance of Cyberspace: Governance structure of cyberspace was discussed, especially, the governance of the logical layer or the domain name system (DNS). The transition of National Telecommunication and Information Administration (NTIA) (of the United States Department of Commerce) stewardship over Internet Assigned Numbers Authority (IANA) functions under the Internet Corporation for Assigned Names and Numbers (ICANN) was briefly discussed. Many States concurred that political consensus is required to manage the critical resources of Internet, where the UN should come forth and play a decisive role.

3) Cyber Warfare: Member States discussed with the guest speaker as to what aspects of and in what manner rules of IHL may be made applicable to cyberspace.

4) Cybercrimes and International Law: Various facets of the Budapest Convention were discussed. Pointing out the lacunae of the Budapest Convention, the guest speaker stated that the "Comprehensive Study on Cybercrime" as carried out by the UNODC could act as better focal point for future endeavors in the form of a regional or global set of model laws. There was a broad agreement between Member States that there needs to exist a set of model laws or even a global convention under the UN for combating cybercrimes, and that the key challenge lies in how this may be achievable.

B. Issues for focused deliberation at the Fifty-Sixth Annual Session of AALCO

1) State Sovereignty in Cyberspace
2) Law and Governance of Cyberspace
3) Cyber Warfare
4) Cybercrimes and International Law

II. Deliberations at the Fifty-Fifth Annual Session of AALCO held in New Delhi, India

5. The Open-ended Working Group on International Law in cyberspace, as per the mandate of the resolution adopted at the Fifty-Fourth Annual Session, met during the Fifty-Fifth Annual Session in New Delhi, India. The meeting began with introductory statements on the topic by the Rapporteur of the Open-ended Working group on International Law in Cyberspace, Prof. Huang Zhixiong, and the then Secretary-General of AALCO, Prof. Dr.

Rahmat Mohamad. Prof. Huang posed a few preliminary questions pertinent to cyberspace, that are currently under the consideration of the international community: a) which part of international law is applicable to cyberspace, b) what should be the rules for maintaining peace and order in cyberspace, and c) how can we more effectively combat cybercrimes based on international law and international co-operation? He also noted that platforms like the present one can help the voices of Asian African countries be heard at this important juncture of development of international law in cyberspace. Next, Prof. Rahmat Mohamad began his speech with identifying and speaking about a few critical issues associated with cyberspace, such as cyberspace having become the "fifth domain" of human-interaction, about the recent international efforts in making the existing "multi-stakeholder" model more equitable and transparent, and about the impending release of Tallinn 2.0, which expands the coverage of Tallinn 1.0 to include peace-time international law. Thereafter, he spoke of the Special Study which is being worked upon by the AALCO Secretariat, and the mandate of the present Open-ended Working Group. Lastly, he invited Member-States to participate in a program that AALCO was hosting at the 25th Session of the Commission on Crime Prevention and Criminal Justice (CCPCJ) at the United Nations Office in Vienna on 23 May 2016, with the theme, "Cybercrimes and International Co-operation: An Asian-African Perspective", with the financial assistance from the People's Republic of China.

6. Delegates from the following Member-States presented their statements on the identified issues relating to "International Law in Cyberspace": People's Republic of China, State of Kuwait, Islamic Republic of Iran, India, Japan, Malaysia, Democratic People's Republic of Korea, and Republic of Korea. Lastly, the representatives from VietNam and the International Committee of the Red Cross also expressed their views as observers on the issue.

7. The delegate from People's Republic of China recalling the mandate of the Working Group, as provided to it at the 54th Annual Session Resolution, stated firstly in respect of international cooperation in combating cybercrimes that it is imperative that AALCO Member-States consider adopting model provisions on cooperation in combating cybercrimes. He stressed on the role of Working Group meetings to achieve that objective, and affirmed support from the Chinese side for the same. Next, with respect to State sovereignty in cyberspace, he stated that State-sovereignty would extend over tangible as well as intangible resources of the Internet, and States ought to respect each other's rights while acting upon their regulation models in cyberspace. With regard to peaceful use of cyberspace, he stated that in the absence of an international consensus in declaring cyberspace as a war domain, application of right of self-defense and rules of armed conflict to cyberspace would aggravate the cyber-arms race and increase the risk of inter-State mistrust. Thereafter, he stressed upon the need of having a global legal framework to combat cybercrimes today and supported the examination of the "comprehensive study on cybercrime" prepared by the UNODC, and also called upon AALCO Member-States to work actively in the direction of developing a global legal framework for combating cyber-crimes. He lastly spoke of the UN Charter as being the main foundation for all further legal endeavors in the realm of cyberspace.

8. The delegate from the State of Kuwait emphasizing on the importance of enhancing international cooperation to effectively combat cyber-crimes, stated the importance of regional Conventions as having made a beginning in that direction. Amongst such Conventions he mentioned the Arab Convention on fighting cybercrimes, which aims to enhance cooperation between Arab States in the area of combating cybercrimes, and which Kuwait ratified in the year 2013 and confirmed to pass national legislations to criminalize acts punishable under it. Thereafter he explained a number of important aspects of the Convention. He also mentioned the endeavor of the European Council in this regard, reflected in the Budapest Convention, and that the Arab Convention mentioned above was ratified in re-iteration and support of it.

9. The delegate from the Islamic Republic of Iran, while attaching high importance to the study of the topic of international law in cyberspace, of its inclusion in the AALCO Agenda, the establishment of the Working Group, as well as the Secretariat's Special Study on it, mainly stressed on whether the present day international law regime is sufficient to meet the challenges posed by the use of cyberspace, or whether there is a need for a new set of rules. He stated that whereas the foundational international law principles do apply to cyberspace, the manner in which they apply is different. He stated how other aspects and principles of international law such as State sovereignty and *sic utere tuo ut alienum non laedas*, should be made to apply to cyberspace as well. With regard to combating cybercrimes, after providing an overview of Iran's law and policy of tackling the issue, he spoke of the major developments in this regard under the leadership of the UN General Assembly, and how Iran has been closely following that. Lastly, he expressed hope towards relevant work in this regard at the AALCO forums.

10. The delegate from India expressed two main concerns which as per its view are being posed by cyberspace today, one, a lack of consensus within the international community on norms of behavior in cyberspace, and two, that the technology continues to remain far ahead of the relevant laws and policies in this regard. He specifically spoke on critical issues of cyber-security (including disagreement on 'use of force' and 'armed attack'), cybercrimes, and issues of jurisdiction over ICT infrastructure, including jurisdiction over such infrastructure located at the high seas, as well as outer space. He also spoke of the growing recognition that international law particularly the UN Charter applies as much to cyberspace, after the recent declaration in this regard by the 2015 UN Group of Governmental Experts (UNGGE). He thus, concluded by emphasizing on the usefulness of forums such as AALCO to arrive at a consensus on the afore-mentioned cyberspace related issues.

11. The delegate from Japan recognizing cyberspace as a driver of social and economic growth, led by the private sector and sustained by the multi-stakeholder model - while supporting the securing of free flow of information in cyberspace, also at the same time stressed on the need to strike a balance between the protection of privacy and assurance of security. With regard to sovereignty issues pertaining to cyberspace, while affirming the view generally held by the international community and also supported by the UNGGE Report of 2015, that '…international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities', he continued to state

that freedom of expression and confidentiality of communication should at the same time be respected and protected. With regard to "Peaceful Use of Cyberspace", he expressed support for taking up confidence building measures (CBM), bilaterally and multi-laterally. Next, with regard to international cooperation in combating cybercrimes, he mentioned the Budapest Convention, the negotiation of which Japan participated in and acceded to in July 2012. He stated that since the Convention is thus far the only effective multilateral instrument in this regard, is based on the universal needs of the practitioners working on cybercrimes, and is relevant with regard to present as well as future technologies, it will benefit the use of cyberspace if more countries harmonize their legislations in the lines of the said Convention. Any efforts under the UN aegis should be careful not to duplicate the provisions already existing in the Convention. Lastly he acknowledged that the existing international law is applicable in cyberspace (though how they apply may need further deliberations), as re-affirmed in the UNGGE Reports.

12. The delegate from Malaysia firstly noted a legal vacuum in respect of State sovereignty in cyberspace. Nevertheless he also took note of the various efforts to address this question internationally, such as at the UN level and at the NATO forum (Tallinn Manual 2.0). He further mentioned that for Malaysia, any exercise of extra-territorial criminal jurisdiction must be based on enabling domestic law. With regard to peaceful use of cyberspace, he agreed that international law, and in particular the UN Charter is applicable. However, he further noted that the applicability of principles of customary international law to cyber disputes may need further examination. Further he stated that a common understanding over the relevant provisions of the UN Charter could fill the existing gaps in the area of international law pertaining to cyberspace. With regard to International Co-operation in Combating Cybercrimes he proposed the harmonization of laws relating to certain cyber offences, which are regular to Member States, as a way forward towards establishing a common international cooperation regime. However, extensive consultation has to go into such legal framework to ensure that such harmonized rules would be acceptable to and practical for all Member States. In this regard he proposed that the Secretariat should conduct a detailed study in this respect that could be later formulated into a set of guidelines. He also stated in this regard that the Budapest Convention needs to be updated from time to time to reflect the changing reality of cyber threats. It may also be expanded into an all-encompassing international cyber treaty. Thereafter he summarized the domestic legal framework in Malaysia that criminalizes cyber-crimes. Lastly he expressed hope at the outcomes of the Working Group deliberations as well as of the Special Study on International Law in Cyberspace, to be released by the AALCO Secretariat, in appropriately guiding the Member-States.

13. The delegate from the Democratic People's Republic of Korea, while condemning acts of cyber warfare and cyber-crimes being conducted world-wide, including State-sponsored ones, which besides causing damage are also more importantly infringing upon the sovereignty of other nations, stated that the UN General Assembly Resolution, "the right of privacy in digital age", adopted at its 69th Session in 2014 is not sufficient to combat cybercrimes due to its non-binding nature. He stated that ongoing efforts to codify international criminal law in cyberspace should stipulate clauses to punish acts of

infringement upon State sovereignty, and to ensure the peaceful use of cyberspace. The DPRK government would fully cooperate and extend support in this regard.

14. The delegate from the Republic of Korea expressing hope for the success of the Working Group stated that with regards to the four issues forming the mandate of the Working Group, activities within the UN, in particular the UNGGE, in this regard needs to be closely followed by the Secretariat and Member-States.

15. The observer delegate from VietNam recognizing cyberspace as a new natural resource like air, water and land, firstly spoke about the fact that nations have sovereign control over ICT resources within their territories, and also the fact that States must also have an extra-territorial jurisdiction over cyber-activities for safeguarding their own interests, while respecting rights of other States in conformity with applicable international law. Next he spoke about steps to be taken in the direction of combating cybercrimes and ensuring cyber-security. After talking about the Vietnamese law on cyber-security he stated the importance of international cooperation in this aspect, including those relating to cyber terrorism, with regard to which VietNam is open to have discussions for further cooperation. Thereafter he condemned all forms of cyber-attacks, and urged all States to cooperate with each other in this regard and also spoke of new initiatives under the aegis of the UN, in formalizing an international instrument covering cyber security.

16. In the end the observer representative from the International Committee of the Red Cross spoke extensively about the threats that cyber-warfare pose in today's date and the importance as well as challenges of applying the rules of International Humanitarian Law to it. He firstly mentioned what includes in the ICRC's understanding of the term, 'cyber warfare', after mentioning that there exists no definition of cyber warfare under international law; notably mentioning that if cyber means are employed during armed conflicts, they must comply with IHL rules like any other means of warfare. Next, he mentioned the unlimited reach of cyber warfare into the civilian world, as one of the reasons and one of the biggest challenges of IHL norms applying to cyber warfare. He spoke of safeguarding essential civilian infrastructure against cyber-attacks, inseparability of military systems from civilian infrastructure, and anonymity in cyberspace, as some of the biggest challenges to the application of IHL norms to cyber warfare. He said that technology will continue to evolve, impacting weapons and warfare. Law too, therefore, will have to evolve to keep up with its pace. ICRC has engaged with a number of States in this aspect, however, how IHL rules are to develop in the future to address challenges of cyber warfare, is something that the States will have to determine. He lastly mentioned ICRC's active support towards such IHL-cyber warfare initiatives such as the Cyber Working Group established as part of the Seoul Defense Dialogue and the present AALCO-led initiative of establishment of the open-ended Working Group in this aspect.

III. Internet Governance and Security in Cyberspace – Recent Developments

A. World Summit on Information Society (WSIS) Forum, 2016

17. The World Summit on the Information Society (WSIS) is a unique two-phase United Nations (UN) summit that was initiated in order to create an evolving multi- stakeholder platform aimed at addressing the issues raised by information and communication technologies (ICTs) through a structured and inclusive approach at the national, regional and international levels. The goal of WSIS is to achieve a common vision, desire and commitment to build a people-centric, inclusive and development-oriented Information Society where everyone can create, access, utilize and share information[1].

18. As per the mandate of the Tunis Agenda, since 2005 a cluster of WSIS-related events have been taking place on an annual basis in Geneva. In 2009, the cluster of WSIS-related events was re-branded as WSIS Forum. With time WSIS Forum has proven to be an efficient mechanism for multi-stakeholder implementation of WSIS Action Lines. WSIS Forums are organized each year, hosted by the ITU, and co-organized by ITU, UNESCO, UNCTAD and UNDP in close collaboration with all WSIS Action Line Facilitators/Co-Facilitators (UNDESA, FAO, UNEP, WHO, UN Women, WIPO, WFP, ILO, WMO, UN, ITC, UPU, UNODC, and UN Regional Commissions)[2].

19. The Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society was held by UN General Assembly in 2015 that adopted Resolution A/70/125 calling for close alignment between the WSIS process and the 2030 Agenda for Sustainable Development, as well as to hold the WSIS Forum on the annual basis till 2025[3].

20. The overall theme of the WSIS Forum 2016, which took place from 2-6 May, 2016, at the ITU headquarters in Geneva, was 'WSIS Action Lines: Supporting the Implementation of SDGs'. The present theme, as well as the theme of the WSIS Forum of last year, was structured along the lines of the afore-mentioned UN General Assembly Resolution A/70/125, 2015, that called for close alignment of the WSIS and SDG process, with due regard to the global mechanism for follow-up and review of the implementation of the 2030 Agenda for Sustainable Development (UNGA Resolution A/70/1). Like the WSIS Forum of 2015, the 2016 Forum too attracted a huge number of stakeholders from various countries, as well as various sectors, both public and private,

[1] The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva from 10 to 12 December 2003 and the second phase took place in Tunis, from 16 to 18 November 2005. In 2003, the number of participants was 11,000 representing 175 countries and in 2005 the number of participants was more than 19,000 representing 174 countries.

[2] WSIS Forum 2016 "WSIS Action Lines: Supporting the Implementation of SDGs: Outcomes", available at: <https://sustainabledevelopment.un.org/content/documents/10186World%20Summit%20on%20Information%20Society%202016%20Outcomes%202016-May-16.pdf>.

[3] *Ibid*.

that provided an ideal atmosphere for the facilitation and exchange on the multi-stakeholder vision of the WSIS Process[4].

21. Moderated High-Level Policy Sessions of the High-level Track (HLT) at the WSIS Forum 2016 took place on the 3rd and 4th of May, 2016. During these sessions, Policy Sessions with high-ranking officials of the WSIS Stakeholder community, representing the Government, Private Sector, Civil Society, Academia and International Organizations were held. Therefore, as has been the case before, this had been a platform to develop multi-stakeholder and public/private partnerships to advance development goals, and it helped co-ordinate multi-stakeholder implementation activities, information exchange, creation of knowledge, sharing of best practices. Policy Sessions were moderated by high-level track facilitators and were grouped around different themes identified as important by the WSIS Stakeholders during the open consultation process and the outcomes of the UN General Assembly Overall Review. In addition, a Ministerial Roundtable provided an opportunity for more than 60 ministers and deputies to discuss national approaches aimed at strengthening the national development plans, and the role of ICTs, in particular WSIS Action Lines, as enablers of the Sustainable Development Goals.[5]

22. High-Level Policy Sessions were divided into fifteen sessions covering fourteen themes. These themes were as follows: WSIS Action Lines and the 2030 Agenda, Bridging digital divides, Enabling environment, Knowledge societies, capacity building and e-learning, Financing for development and role of ICT, Building confidence and security in the use of ICTs, Inclusiveness – access to information and knowledge for all, Gender mainstreaming, ICT applications and services, Digital economy and trade, Climate change, Media, Ethical dimensions of Information and Knowledge Societies, Cultural diversity and heritage, linguistic diversity and local content[6].

B. Expiration of the IANA Functions Contract

23. With the Internet Assigned Numbers Authority (IANA) functions contract of the U.S Government having officially expired on 1st October, 2016, the co-ordination and management of the Domain Name System is now privatized and in the hands of the volunteer-based multi-stakeholder community. On 14 March 2014, the U.S. National Telecommunications and Information Administration (NTIA) had announced its intent to transition its stewardship of the IANA functions to the global multi-stakeholder community[7].

[4] *See generally* 2016 WSIS Forum website, available at: <https://www.itu.int/net4/wsis/forum/2016/About/>.
[5] "WSIS Forum Outcome Document", 2-6 May, 2016, Geneva, Switzerland., available at: <https://www.itu.int/net4/wsis/forum/2016/Outcomes/#ft>.
[6] "WSIS Forum 2016: High Level Track Outcomes and Executive Brief", 2-6 May, 2016, Geneva, Switzerland, available at: <https://www.itu.int/net4/wsis/forum/2016/Outcomes/#ft>.
[7] *See generally* ICANN's website, available at: <https://www.icann.org/stewardship>.

24. The transitioning stewardship of the IANA functions to the multi-stakeholder community marks the final phase of the privatization of the DNS as outlined by the 1998 White Paper. It symbolizes the end of a nearly 20 year old journey toward a fully realized model of global governance of the technical management of the Internet names, addresses and protocol parameters.

25. At the 55th Public Meeting of ICANN in March 2016 in Morocco, ICANN received proposals for the transition of the IANA functions from the US Department of Commerce's National Telecommunications and Information Administration (NTIA) to global Internet stakeholders and to enhance ICANN's accountability[8]. Volunteers representing a broad range of interests from the multi-stakeholder Internet community had developed these proposals. NTIA – working with other U.S. Government agencies – reviewed the transition proposals to ensure they met the criteria NTIA outlined in its March 2014 announcement. On 9 June 2016, NTIA announced that the proposals met the criteria. The acceptance of the proposals was an important milestone toward completing the transition and ensuring that the Internet remains a platform for innovation, economic growth and free speech[9]. As a result the U.S Government formally gave up its stewardship of key Internet technical functions, making ICANN accountable as a fully independent organization, and placing the coordination and management of the Internet's unique identifiers in the hands of the volunteer-based global Internet community. The IANA functions will now be provided greater visibility through their embodiment in the Public Technical Identifier's subsidiary.

26. Along with the stewardship transition including the largest-ever expansion of available top-level domains through the New generic Top-Level Domain Program (gTLD). Today, more than 1,000 new gTLDs from the 2012 application window have been introduced into the Internet. There are now nearly 50 times as many gTLDs as there were in 2013.

27. In addition the year 2016 saw a marked increase in the number of governments that joined the Governmental Advisory Committee (GAC) and in the levels of participation by countries at ICANN meetings[10]. This participation strengthens participation by governments in and support for the Internet governance ecosystem using a multi-stakeholder approach[11].

---

[8] ICANN's Annual Report 2015-16, available at: <https://www.icann.org/resources/pages/governance/annual-report-en>.

[9] The plan, formally known as the IANA stewardship transition, had to meet the following criteria:

- Support and enhance the multi-stakeholder model
- Maintain the security, stability and resiliency of the Internet Domain Name System (DNS)
- Meet the needs and expectations of the global customers and partners of the IANA services
- Maintain the openness of the Internet

[10] In FY16 15 additional countries have become members of ICANN's GAC: Antigua and Barbuda, Belize, Guyana, Haiti, Honduras, Panama, Suriname, Burundi, Chad, Palestine, Republic of the Congo, Sierra Leone, Cambodia, the Republic of Palau and Tokelau. In addition four regional groups, the Caribbean Telecommunications Union (CTU), the Organization of Eastern Caribbean States (OECS), the West Africa Telecommunications Regulators Assembly (WATRA) and the Economic Community of Central African States (ECCAS) have joined the Committee as observers.

[11] ICANN's Annual Report 2015-16, p. 53, available at: <https://www.icann.org/resources/pages/governance/annual-report-en>.

C. Tallinn Manual 2.0

28. The "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", as the name suggests, is an updated and considerably expanded second edition of the 2013 "Tallinn Manual on the International Law Applicable to Cyber Warfare". The new book offers a fascinating look at how far the cyber threat landscape has evolved in the less than half decade since the first version's release in 2013, shifting the focus from conventional state-authorized and operated cyber warfare to the more common cyber incidents that States encounter on a day-to-day basis and that fall below the thresholds of the use of force or armed conflict.

29. The manual is essentially a massive 642 page narrative on the legal landscape of cyber today. It presents a myriad of legal questions that commonly arise in cyber operations and discusses the current state of international law and how it might apply to each given scenario. In many cases the drafters were unable to reach a consensus, illustrating the complexities and vagaries that still plague the cyber world[12].

30. Following the format of the original Tallinn Manual (Tallinn Manual 1.0) the Experts have adopted additional rules that have been added to the original ones to produce "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations". Accordingly, Tallinn Manual 2.0 supersedes the first Tallinn Manual. As was the case with the first Tallinn Manual, the primary audience of Tallinn Manual 2.0 is also meant to be the State legal advisers who provide civilian and military international law advice to the governmental decision makers. However, the makers of the Tallinn Manual 2.0 are also hopeful for its academic value[13].

31. The rules and commentary of the Tallinn Manual 2.0, which it draws from the Tallinn Manual 1.0 addresses two subjects: *jus ad bellum* and *jus in bello*. The remainder deals with key aspects of public international law governing cyber-operations during peacetime. Therefore, the 2017 edition covers a full spectrum of international law as applicable to cyber operations, ranging from peacetime legal regimes to the law of armed conflict. However, the aspect of peacetime legal regime has not been comprehensively dealt with in the Manual. For instance, the Manual does not deal with international criminal law, trade law, intellectual property, private international law or domestic law. Topics included comprise of a wide array of international law principles, and include principles of general international law, such as the sovereignty and the various bases for the exercise of jurisdiction. The law of state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialized

---

[12] *See generally* the NATO Cooperative Cyber Defense Centre of Excellence's site, available at: <https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html>. *See also*, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Factsheet", NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia (2017), available at: <https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf>.

[13] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, (CUP, 2017), pp. 1-7.

regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law are examined within the context of cyber operations[14].

32. Notwithstanding that only few treaties presently directly deal with cyber-operations, that those that have been adopted are of a limited scope, and that it is presently difficult to definitively identify any cyber-specific customary international law, the 'Introduction' to the Tallinn Manual 2.0 mentions that both the International Groups of Experts have been unanimous in their estimation that existing international law applies to cyber-operations. Accordingly, therefore, both versions of the Tallinn Manual have determined how the identified aspects of international law apply in the cyber-context, and to identify any cyber-unique aspects thereof[15].

33. Tallinn Manual 2.0, as the first Tallinn Manual is not an official document, but rather the product of two separate endeavors undertaken by groups of independent experts acting in their personal capacities. The manual does not represent the views of the NATO CCDCOE, NATO, or any other country whose expert was involved in the framing of the present manual. Also, the Manual is an objective re-statement of the law as it existed at the time of the Manual's adoption (*lex lata*). It is not meant to be a best practices guide, representative of the 'progressive development of law, or indicative of *lex ferenda*. It is also meant to be politics and policy-neutral[16].

D. Nineteenth Session of the Commission on Science and Technology for Development

34. Since 2006 the UN's Commission on Science and Technology for Development (CSTD), which is substantially serviced by the UNCTAD and is a subsidiary body of the Economic and Social Council (ECOSOC), has been mandated by ECOSOC to serve as the focal point in the system-wide follow-up to the outcomes of the World Summit on the information Society (WSIS) and advise the Council thereon.

35. One of the two priority themes of the Nineteenth Session of the CSTD that took place from 9-13 May, 2016, in Geneva, Switzerland, was "Foresight for Digital Development", in which the Commission reviewed the progress made in the implementation of the outcomes of the World Summit on the Information Society (WSIS).

36. In the review process the participants highlighted both the positive as well as the negative aspects of the implementation process. On the one hand they spoke about the rapid growth in access to mobile technology and broadband since 2005 which has meant that more than half of the world's inhabitants should have access to ICTs within their reach and make use of them by the end of 2016, in line with one of the World Summit targets, while reaffirming their commitment to the full implementation of the outcomes and the

[14] Ibid.
[15] *Id*, p. 3.
[16] Tallinn Manual 2.0, n 13.

World Summit vision beyond 2015. On the other hand they also noted with great concern that many developing countries lacked affordable access to ICTs and that, for the majority of the poor, the promise of science and technology, including ICTs, remained unfulfilled. Consequently, participants emphasized the importance of promoting an inclusive information society, with particular attention given to bridging the digital divide and broadband divide, taking into account the considerations of developing countries, gender and culture, as well as youth and other underrepresented groups. [17].

37. In considering the priority theme "Foresight for digital development", the expert panel analyzed foresight for policymaking on science, technology and innovation and addressed the development implications of four emerging digital developments, namely, big data and the "Internet of things"; three-dimensional printing (also known as additive manufacturing); automation of work; and massive open online courses.

38. During the discussion participants called on Governments, individually and collectively, to put in place policies that support the development of digital ecosystems that are inclusive and take into account the socioeconomic and political context of countries. In particular in the context of the 2030 Agenda for Sustainable Development, Governments were encouraged to undertake systemic research, including foresight exercises, on new trends in science, technology and innovation, and information and communications technologies and their impact on development.

IV. Comments and Observations of the AALCO Secretariat

39. Various aspects of international law in cyberspace are being actively discussed on multiple significant international and regional forums around the world today. Global governance in terms of the major issues, namely State sovereignty, cyber-crimes, peaceful uses of cyberspace, application of international law in cyberspace, and governance of the Domain Name System as well as other policy matters, has come a long way owing to significant efforts that has been put in this direction by the international community.

40. The international community also witnessed some positive developments in the cyber-sphere in the span of the last one year. The transition of the IANA functions from the stewardship of the NTIA, for example, onto the hands of the global multi-stakeholder community, is one of the most significant milestones in the journey towards achieving a fully realized model of global governance of the technical management of the Internet names, addresses and protocol parameters. Furthermore, an increased participation in the GAC of the ICANN reflects a step towards a more inclusive participation in the technical regulation of Internet. How the IANA functions would be managed within ICANN now, however, remains to be seen.

[17] *Commission on Science and Technology for Development: Report on the Nineteenth Session (9-13 May 2016),* Economic and Social Council, Official Records, 2016, Supplement no. 11 (E/2016/31-E/CN.16/2016/4).

41. The WSIS Forum 2016 has worked further towards realizing an inclusive multi-stakeholder approach for cyber-governance. Discussions over the WSIS Forum as well as the UNCSTD have made progress in the direction of closely aligning digital development with 2030 Agenda for Sustainable Development, and bridging the digital divide.

42. The AALCO Secretariat also notes with interest the work of the International Group of Experts, working under the NATO CCDCOE, to publish their substantial work relating to the applicability of the peace time legal regime to cyberspace, in the form of Tallinn Manual 2.0. The Tallinn Manual 2.0 shifts the focus from the conventional State-authorized and operated cyber warfare to the more common cyber incidents that States encounter on a day-to-day basis. Even though an unofficial document, the Tallinn Manual 2.0 contributes significantly to the existing scholarship, and features as an important stepping stone that could help to form and develop binding legal rules in this regard.

43. Over the previous discussions that have taken place on this issue at the forums of AALCO, many of the Member States have come out in favor of having uniform binding rules of international law under the aegis of UN, affecting various facets of cyberspace, such as State-sovereignty, cyber-crimes and applicability of IHL rules in cyberspace, for lesser conflicts and better governance within the realm of cyberspace.

44. The AALCO Open-ended Working Group on International Law in Cyberspace and the Secretariat would be guided by the collective wisdom of Member States in their future endeavors as well as on deciding the final outcome of their present mandates in this regard, including the possible drafting of a set of model laws on combating cybercrimes. The Secretariat further recommends the Member States to follow closely the international events in this regard – participating and providing their valuable inputs therein. It also urges them to cooperate with the Secretariat in all its future undertakings, to come up with solutions to the present problems and fill in the existing lacunae in the realm of cyberspace.

ANNEX

SECRETARIAT'S DRAFT
AALCO/RES/DFT/56/S17
5 MAY 2017

INTERNATIONAL LAW IN CYBERSPACE

The Asian-African Legal Consultative Organization at its Fifty-Sixth Session,

Having considered the Secretariat Document No. AALCO/56/NAIROBI/2017/SD/S17,

Noting with appreciation the introductory statement by the AALCO Secretariat,

Welcoming the Special Study on the topic prepared by the AALCO Secretariat,

Welcoming also the Summary Report of the Chairperson of the Open-ended Working Group on International Law in Cyberspace, on the 2nd Meeting of the Open-ended Working Group on International Law in Cyberspace, held at AALCO Secretariat, New Delhi, on 9 and 10 February, 2017,

Recognizing the significance of cyberspace as an integral part of human interaction and its profound impact on Member States and their citizens,

Recognizing also the urgency to prevent the use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security,

Realizing the need to develop a transparent and balanced global mechanism for the governance of the Internet in pursuance of equity and bridging the "digital divide" existing among States,

Deeply concerned about new threats and challenges in the development and application of information and communication technologies such as cybercrimes, cyber-warfare and the use of cyberspace for terrorist purposes,

Noting with concern the escalation in various kinds of cyber-attacks perpetrated by State and non-State actors,

Realizing especially the need for enhanced coordination and judicial cooperation among Member States in combating the criminal misuse of information and communication technologies,

Stressing the significance of the principles and rules of international law applicable to cyberspace, including those in the UN Charter,

Also stressing the urgent need for further development of rules of international law on cyberspace issues,

1. **Encourages** Member States to actively participate in the relevant regional and global forums deliberating on the governance of cyberspace and to strengthen their communication and cooperation in this regard;

2. **Directs** 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;

3. **Directs** the Secretariat to closely follow developments in international forums related to governance of cyberspace and cyber security, and to organize open-ended Working Group meetings, as and when necessary, depending upon the availability of finances, preferably in collaboration with Member States, international organizations or other institutions; and

4. **Decides** to place this item on the provisional agenda of the Annual Session as and when required.