AALCO/55/NEW DELHI (HEADQUARTERS)/2016/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

(Deliberated)

CONTENTS

Pages

I. Introduction **1-2**

A. Background
B. Issues for focused deliberation at the Fifty-Fifth Annual Session of AALCO

II. Deliberations at the Fifty-Fourth Annual Session **2-5**

III. Internet Governance and Security in Cyberspace- Recent Developments **5-10**

A. World Summit on the Information Society (WSIS) Forum, 2015
B. The 54th Meeting of the Internet Corporation for Assigned Names and Numbers (ICANN)
C. 10th Annual Internet Governance Forum
D. WSIS +10 Review
E. Tallinn 2.0

IV. Comments and Observations of the AALCO Secretariat **10-11**

V. Annex **12-13**
Draft Resolution

INTERNATIONAL LAW IN CYBERSPACE

I. Introduction

A. Background

1. Cyberspace is a ‘‘borderless’’ world—computer-based communications cut across territorial borders creating a new realm of human activity. According to the International Telecommunication Union (ITU), globally 3.2 billion people are using the Internet at end of 2015, of which 2 billion are from developing countries.[1] Between 2000 and 2015, global Internet penetration grew seven fold from 6.5% to 43%.[2] Governments, businesses, and organizations in civil society are increasingly using information and communication technology (ICT) platforms as tools of communication and governance. Despite evolving into one of the most preferred platforms for the communication of information and delivery of plethora of services, the unique attributes of cyberspace pose considerable challenges in formulating standardized rules to effectively regulate interactions in the Internet.

2. Firstly, and more generally, the formulation and enforcement of international legal norms, be it by way of multilateral treaties or by developing rules of customary international law, lags behind technological developments taking place in ICTs. This difficulty is compounded by the slow progress in the multilateral efforts to establish binding norms for governing cyberspace. For instance, in the ITU Plenipotentiary Conference 2014, held in Busan, Republic of Korea, it was expected that ITU would be mandated with a greater role in Internet governance.[3] However, this did not materialize due to strong objections mostly from a few developed nations preferring the retention of the existing multi-stakeholder model. Secondly, increasing frequency of cyber attacks and transnational cybercrimes poses novel challenges to traditional international law. Because attribution is difficult in a digital context, identifying and holding accountable actors in cyberspace is challenging if not impossible. Another hurdle is insufficient law enforcement cooperation between States.

3. It is broadly in this context that People’s Republic of China, in accordance with AALCO Statutory Rules, proposed “International Law in Cyberspace” as an agenda item to be deliberated at the Fifty-Third Annual Session of AALCO held in Tehran in 2014 and it was accepted by consensus. The agenda item was also deliberated in the Fifty-Fourth Annual held in Beijing, China in 2015. The Resolution on the agenda item adopted in the 2015 AALCO Annual Session directed the Secretariat to study this subject based on deliberation and progress made in the UN framework and other forums, with special attention to international law pertaining to State Sovereignty in cyberspace,

[1] International Telecommunication Union, *ICT Facts and Figures*, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
[2] Ibid.
[3] Monika Ermert, ITU Plenipotentiary Conference: Internet Governance Diplomacy on Display, available at http://www.ip-watch.org/2014/11/05/itu-plenipotentiary-conference-Internet-governance-diplomacy-ondisplay/

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. This study is due to be released in the upcoming Annual Session scheduled to be held in New Delhi in May 2016. Since the study comprehensively covers the international regime applicable to cyberspace and elaborates associated legal challenges, this brief shall only concentrate on enlisting and explaining the international developments in cyber governance and security in cyberspace occurred since the conclusion of the previous Annual Session in Beijing in April 2015.

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

1) International law pertaining to state sovereignty in cyberspace;

2) Peaceful use of cyberspace;

3) Rules of international cooperation in combating cybercrimes, and

4) Identification of the relevant provisions of the UN Charter and other international instruments related to cyberspace.

4. Further, it may be recalled that the Member States, through the resolution adopted on this Agenda Item in Fifty-Fourth Annual Session held in Beijing (AALCO/RES/54/SP2), established an open-ended working group on international law in cyberspace to discuss the abovementioned issues as identified in operative paragraphs of the resolution.

5. It is proposed that the open-ended working group, in its first meeting during the Fifty-Fifth Annual Session of AALCO, (1) elect the Chair, Vice-Chair and Rapporteur of the Working Group, according to the stipulation in Rule 14 (2) of AALCO Statutory Rules; (2) deliberate on the aforementioned issues in their interventions; and (3) discuss possible final outcome of consideration on this topic or its general direction.

II. Deliberations at the Fifty-Fourth Annual Session held in Beijing, People's Republic of China

6. A Half Day Special Meeting on "International Law in Cyberspace" was held during the Fifty-Fourth Annual Session in Beijing, People's Republic of China. Two experts on the topic were invited as panelists for this meeting. The meeting began with the introductory statement on the topic by the Deputy Secretary General of AALCO, Mr. Feng Qinghu emphasizing on the new challenges which include: (1) disagreement over a universally accepted structure of internet governance and associated issues including state sovereignty in regulating internet within its jurisdiction, (2) articulation of rules related to state and non-state conduct during cyber warfare, and (3) burgeoning transnational cyber crimes and the need for a multilateral treaty to effectively prevent its escalation. With regard to cyber warfare, he noted that the articulation of traditional rules of war, both on the use of force (*jus ad bellum*) and International Humanitarian Law (*jus in bello*), applicable to cyberspace is a prime concern. While noting that cyber espionage factors have become a critical concern with respect to cyber security, he emphasized that Vienna Convention on Diplomatic Relations reaffirmed the inviolability of diplomatic correspondence and that it equally applied to cyberspace as well. As regards cybercrimes

and international law, he added that its provisions did not adequately address various new threats such as terrorist use of the Internet, botnet attacks and phishing.

7. Mr. Zhijong Fan, Representative of HUAWEI, explained the various ways in which Internet has changed our lives taking into account the past, present and future of the Internet. He stated that protecting Internet and preventing its misuse is as vital as protecting other sources such as air and water and that the misuse of the Internet would only undermine the efforts of mankind and slow down the technology evolution itself.

8. Mr. Richard Desgange, Regional Legal Advisor, ICRC, Beijing explained why it has been difficult to provide an authoritative definition of 'cyber warfare' and stressed that International Humanitarian Law (IHL) applies to this new technology in armed conflicts. He went on to add a list of challenges emanating from the interpretation and application of IHL in regard to cyberspace. Firstly, since IHL relies on attribution of responsibility to parties to an armed conflict, anonymity in cyber space may create major legal challenges. Secondly, in cases where the only hostile act is a cyber-operation, it may be difficult to call it an armed attack within the meaning of IHL. This question was closely related but nevertheless distinct from whether a cyber-operation alone could amount to a "use of force" or an "armed attack" under the UN Charter. Thirdly, the interconnectedness of cyberspace makes it impossible to distinguish between military and civilian networks before launching cyber-attacks.

9. The following delegates of Member States presented their statements pursuant to the presentations made by the panelists: People's Republic of China, Japan, Republic of Korea, Kenya, Islamic Republic of Iran, Malaysia, India, Nepal, South Africa, Pakistan, Democratic Republic of Korea, Sultanate of Oman and Sudan.

10. The delegate of China, in his statement, pointed out that the orderly functioning of cyberspace concerns the interests of all States which should not be appropriated by any single State. Each State is entitled to exercise sovereignty over cyber infrastructure, network data, cyber activities and Internet governance within its territory. Each State may also exercise extra-territorial jurisdiction over cyber activities pursuant to international law. China also acknowledged the importance of States fulfilling their obligations emanating from sovereignty. It also stated that some States are exaggerating the level of cyber attacks by categorically describing cyber attacks as cyber warfare, invoking the provisions of the Charter of the United Nations on the threat of use of force or armed attack, and advocating the application of *jus ad bellum*, *jus in bello*, and in the law of State responsibility to cyber attacks. The delegate of China also stated that Budapest Convention on cybercrimes has its drawbacks— first, many concerns of developing States have not been taken into consideration, and second, provisions in the Convention that States may conduct cross-border investigation without the consent of the territorial State would jeopardize the judicial sovereignty of a State. Therefore, the delegate stated that the Chinese side supports negotiating an international convention on combating cyber crime under the framework of the United Nations.

11. The delegate of Japan stated that it is essential to maintain an open and transparent environment based not on multilateral, but multi-stakeholder approaches that all

stakeholders, such as civil society, academic, private company, NGO and government should participate in the process. As regards militarization of cyberspace, States are encouraged to take confidence-building measures (CBM) bilaterally and multilaterally to prevent unintended escalations that are not intended by parties. He pointed out that Japan is currently the only Party from the Asian region to Budapest Convention and believes that if more countries harmonize their domestic legislations to the standard of the Convention, it will contribute greatly to the stable use of cyberspace.

12. The delegate of Republic of Korea stated that given the unique characteristics of cyberspace, States need to be realistic and cautious in developing ideas for international governance of cyberspace. He also pointed out at the importance of examining the existing rules of international law to activities of States and non-state actor in cyberspace.

13. The delegate of Kenya spoke about the efforts of East African States to effectively address emerging challenges in cyberspace and pointed out that African Union has developed Convention on Cyber Security and Personal Data Protection, which addresses cyberspace-related matters, including data-protection and the prevention of cybercrimes in line with the increasing adoption of similar legislations in other parts of the world.

14. The delegate of Malaysia stated that his country recognizes the importance of balancing sovereign rights of the States and fundamental freedoms of speech and expression in cyberspace. He also stressed on the need to forge international instruments to ensure that the international community is well equipped to combat cyber crimes.

15. The delegate of Islamic Republic of Iran reminded that serious efforts are needed to amend the current system provided by Internet Corporation for Assigned Names and Numbers (ICANN). He also stated that Iran believes that the first step in curbing cyber-attacks is the exercise of sovereignty by every single State, within its borders, without supremacy given to a single State by way of unlimited powers over cyber activities of other States. He also pointed out that the rules of International Humanitarian Law, i.e. rules derived from The Hague Regulations of 1907, or Geneva Conventions of 1949, do apply to cyber-attacks launched during military operations. He also stated that Iran is of the view that despite the impossibility of creating a new treaty system from whole cloth to regulate cyber-warfare, dealing with details would require, without doubt, hard work on the part of all States and specifically AALCO Member States.

16. The delegate of India stressed on the relevance of the UN Charter and its applicability to various aspects of cyber security. He also pointed out that there is no consensus as to the precise threshold at which cyber operations amounts to an internationally wrongful threat or use of force. Further, he pointed out that the Budapest Convention has been criticized as being fundamentally unbalanced and its long term effectiveness has been brought into question on numerous occasions.

17. The delegate of Nepal also reminded the Member States of the significance of the UN Charter in transnational activities in cyberspace and urged AALCO Member States to study and discuss the issue comprehensively.

18. The delegate of South Africa stressed on the fact that cyberspace is neither immune from State sovereignty nor can it be considered a global commons. She reminded the Member States that combating cybercrime effectively requires global cooperation involving a broad group of countries.

19. The delegate of Qatar spoke about the legislative and institutional efforts of his State to combat cyber incursions and cybercrime. He also discussed the national strategy of Qatar to ensure security in cyberspace.

20. The delegate of Pakistan said that his State respects the right to freedom of expression and right of privacy in cyber space. He also emphasized that the sovereign rights of States in cyberspace need to be respected.

21. The delegate of Democratic People's Republic of Korea (DPRK) stated that the United States, taking the advantage of its monopoly position in cyberspace is diverting the use of cyberspace from serving the sound advancement of humankind, and slandering and disturbing the social and political stability of other independent countries. He also stated that DPRK regards that State sovereignty should be definitely secured in the use of cyberspace and rejects all forms of cybercrimes on the internet.

22. The delegate of Oman repeated his request for adoption of an AALCO Resolution stating the need for an international convention to comprehensively dela with legal issues in this area.

23. The delegate of Sudan stressed on the importance of judicial cooperation in ensuring security in cyberspace. He also spoke about the legislations adopted by Sudan in combating cybercrimes.

24. The Resolution (AALCO/RES/54/SP2) adopted pursuant to the deliberations stressed on the significance of the principles of international law applicable to cyberspace, including the UN Charter and the need for further development of rules of international law on cyberspace.

III. Internet Governance and Security in Cyberspace—Recent Developments

A. World Summit on the Information Society (WSIS) Forum, 2015

25. The World Summit on the Information Society (WSIS) is a pair of United Nations-sponsored conferences about information, communication and, in broad terms, the information society that took place in 2003 in Geneva and in 2005 in Tunis.[4] One of its chief aims was to bridge the global digital divide by spreading access to the Internet in the developing world. The WSIS Follow Up aims at and works towards achieving the indicative targets set out in the Geneva Plan of Action and serve as global references for improving connectivity and universal, ubiquitous, equitable, non-discriminatory and affordable access to, and use of, ICTs, considering different national circumstances, to be achieved by 2015, and using ICTs, as a tool to achieve the internationally agreed development goals and objectives, including the Millennium Development Goals.[5] Since

[4] *See generally* World Summit on the Information Society, http://www.itu.int/net/wsis/
[5] World Summit on the Information Society, http://www.itu.int/net/wsis/follow-up/index.html

2006 the WSIS Forum has been held in Geneva around World Information Society Day (17 May) to implement the WSIS Follow Up. The event is organized by ITU, UNESCO, UNCTAD and UNDP and hosted by the ITU.

26. The WSIS Forum 2015 was held from the 25 to 29 May 2015 at the ITU Headquarters in Geneva. The Forum attracted more than 1800 stakeholders from more than 140 countries. The sessions and discussions supported the WSIS Forum 2015 theme of *Innovating Together: Enabling ICTs for Sustainable Development*. The discussions centered on ICT and its growth and impact in an increasingly hyper-connected world, focusing on progress that has been made on implementation of WSIS Outcomes and discussing the current challenges and challenges that may lie ahead as technology advances at tremendous speed.[6]

27. In the various panels and discussions, multi-stakeholder collaboration across borders and among industries and communities was stressed. Also, Internet of Things (IoT), in the context of being a significant driver in revolutionizing the application of the Internet, was discussed in multiple forums. Cyber security was also a significant part of the dialogue during the Forum, with several sessions organized on the topic. Further, through the series of policy statements, the need for multi-stakeholder model of cooperation to bridge the digital gap, particularly to connect rural areas, was stressed. Other themes included the need for affordable access to ICTs, the encouragement for innovation, the inclusivity of the Internet and the applicability of ICTs in cyber security.[7]

28. Significantly, there was an emphasis on linking the WSIS process with sustainable development. To showcase the impact of ICTs for sustainable development, a document that maps the WSIS Action Lines with the proposed UN Sustainable Goals was issued during the conference.[8] This document draws direct linkages of the WSIS Action Lines with the proposed SDGs to continue strengthening the impact ICTs for sustainable development.

B. The 54th Meeting of the Internet Corporation for Assigned Names and Numbers (ICANN)

29. The 54th meeting of the Internet Corporation for Assigned Names and Numbers (ICANN 54), the global body that oversees the technical and functional workings of the Internet, took place in Dublin, Ireland on 18-22 October 2015. ICANN meetings provide the opportunity for an internationally diverse group of individuals and organizations to come together and discuss and develop policies for the Internet's naming systems. As is well known, ICANN, an international non-profit private body headquartered in Los Angeles, is responsible for assigning the numbers that comprise Internet Protocol (IP) addresses. It also has responsibility for ensuring that users arrive at the same online destination, regardless of the country they are located in or the Internet service provider they use. Since 1998, ICANN has assumed these responsibilities with the oversight of the

[6] http://www.itu.int/net4/wsis/forum/2015/Outcomes/

[7] http://www.itu.int/net4/wsis/forum/2015/Content/doc/outcomes/WSISForum2015_OutcomeDocument_ForumTrack.pdf

[8] The document is available at http://www.itu.int/net4/wsis/sdg/

United States Department of Commerce. There have long been calls for the United States to relinquish this role, and in 2014, the U.S. indicated that it would be prepared to do so as long as ICANN does not come under the control of any intergovernmental or government-led body.[9]

30. Perhaps inevitably, the issue of transition dominated every conversation held at ICANN 54. The core question for ICANN 54 was how to ensure that ICANN can independently exercise stewardship of the Internet's domain name system at the same time remaining accountable to the global Internet community. The responsibility for drafting a proposal to manage the technical transition process as the Internet Assigned Numbers Authority[10] (IANA) functions move away from U.S. oversight to global stakeholders fell to the IANA Stewardship Transition Coordination Group (ICG), which represents Internet stakeholder groups.

31. Although there is widespread agreement among stakeholders that the Internet must be a safe place for users to conduct business and to exchange ideas, it has been difficult to reach a similar consensus about how ICANN's own governance and accountability should be measured. As a result, a working group was established in 2014 to enhance ICANN's accountability. At ICANN 54, the group's co-chair, León Sanchez, announced a 10-point plan that seeks to preserve ICANN's existing consensus-based decision-making model whilst allowing the organization to retain absolute authority over the world's communications protocols.[11] At the heart of the proposal is a shift to a 'sole delegator' model that imposes procedural restrictions on ICANN staff and empowers the global Internet community with meaningful sanctions intended to provide a check on power.[12]

32. The Meeting also included discussions of issues around the new generic top-level domains (gTLD) programme, which was developed to increase choice in the domain name marketplace. As the Internet enters a new phase in its development, this programme will have an increasingly important role to play in how online geo-political power is distributed, and so discussions in this area are important. The Non-Commercial Users Constituency (NCUC), which provides civil society with a voice in ICANN's activities, reflected on the successes and challenges brought about by the first round of the new programme. The original ICANN by-laws called for the development of a competitive, market-based system for the registration of domain names, but as the new gTLD programme expands, the NCUC says that clearer guidelines must be implemented to

[9] See *NTIA Announces Intent to Transition Key Internet Domain Name Functions*, United States Department of Commerce, https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-Internet-domain-name-functions

[10] IANA is a department of ICANN that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers.

[11] https://www.icann.org/news/blog/cross-community-working-group-on-enhancing-icann-accountability-icann54-co-chairs-statement

[12] Ibid.

ensure that no generic names are restricted from public sale under the guise of protecting intellectual property rights.[13]

C. 10th Annual Internet Governance Forum

33. The Internet Governance Forum (IGF) is one of the most critical outcomes of WSIS. The second phase of WSIS, held in Tunis in November 2005, formally called for the creation of the IGF and set out its mandate.[14] It is a multi-stakeholder forum for policy dialogue on issues of Internet governance. The approach of the IGF is straightforward—anyone who has a stake in the future of the Internet can go and be heard. It was founded and operates on the principles of transparency and inclusiveness and seeks to bring together diverse voices and experts in a bottom-up and inclusive fashion to address plethora of challenges in governing the Internet. The establishment of the IGF was formally announced by the United Nations Secretary-General in July 2006. It was first convened in October–November 2006 and has held an annual meeting since then.

34. The 10th annual Internet Governance Forum was held from November 10-13, 2015 in João Pessoa, Brazil The overarching theme for the meeting was: "Evolution of Internet Governance: Empowering Sustainable Development." The event reportedly succeeded in giving some 4,000 online participants, from 116 developed and developing countries, the opportunity to engage directly with 2,400 on-site attendees in debates that addressed the challenges, as well as opportunities for the future of the Internet.[15]

35. The Forum emphasized the importance of ICTs and the Internet to the achievement of the recently adopted 2030 Agenda for Sustainable Development. Over 150 thematic workshops at the 10th IGF focused on a diverse range of topics spanning from zero rating and network neutrality to freedom of expression online, cyber security and Internet economy. Many workshops stressed the interrelation of human rights and fundamental freedom both online and offline and how this related to the promotion of development. One pressing issue was the online risks that children face. Privacy issues were also part of the discussions: it was stressed that encryption and anonymity needed to be reinforced and agreements on the need for privacy, transparency and security issues had to complement and not compromise each other. The need for a secure Internet to foster development was addressed with many participants calling for public-private partnerships.[16]

---

[13] Ayden Ferdeline, *As ICANN 54 Ends, More Uncertainty over the Future of the Internet,* lse.ac.uk/mediapolicyproject/2015/11/10/as-icann-54-ends-more-certainty-over-the-future-of-the-Internet/

[14] Tunis Agenda for the Information Society, paras 29-82, World Summit on the Information Society, United Nations, 18 November 2005

[15] *See* Press Release, https://www.intgovforum.org/cms/press/igf2015-press/549-final-press-release-igf2015/file

[16] http://www.un.org/apps/news/story.asp?NewsID=52559#.VwJUVZwrJH1

D. WSIS +10 Review

36. In December 2015, the United Nations General Assembly reviewed if the WSIS goals progressed over the past ten years and considered the future of the WSIS process beyond 2015. This was often called the "WSIS+10 Review" and culminated in a High-Level Event from 15-16 December 2015 at the UN Headquarters in New York. The Review marks the ten-year milestone since the WSIS, two-phase summit (2003-2005) that defined the issues, policies and frameworks to address ICTs to foster development. The review concluded successfully with the adoption of the WSIS+10 Resolution on 16 December 2015. The review process was described as a 'diplomatic sprint'— in just a few months (effectively since September 2015), negotiators managed to draft a complex and diplomatically delicate text.[17] Almost half of the WSIS+10 Resolution covers digital development.[18] In addition, the Resolution has a strong link with the 2030 Agenda for Sustainable Development. As the ITU's matrix shows, all of the 17 sustainable development goals rely on digital technologies in the implementation process.[19]

37. While WSIS+10 reached rough consensus on development, security, and human rights issues, as regards the topic of Internet governance, the main division between the inter-governmental and the multi-stakeholder approaches to Internet governance remained alive.[20] Overall, however the agreed outcome document represents a positive vision by re-committing to the Tunis Agenda and the principle of a multi-stakeholder model for Internet governance.[21] Recognizing the role that the IGF plays, the WSIS+10 outcome document renews its mandate for ten years. It also asserts that human rights in cyberspace must be protected as they are offline. The text also recognizes the responsibility of Member States to ensure cyber security and stresses the importance of effective stakeholder participation in this regard**.**

E. Tallinn 2.0

38. Even though cyberspace emerged as the "fifth domain" to engage in hostilities, many States and legal experts have argued that the international landscape was premature for a comprehensive international agreement to govern international security in cyberspace.[22] This necessitates the determination of the applicability of existing international law to cyberspace. The United Nations Group of Government Experts (UNGGE) on cyberspace

[17] *Rough Consensus & Ambigious Compromise in Global Digital Politics,* http://www.huffingtonpost.com/entry/rounh-consensus-ambigious_b_8848952.html?section=india
[18] *See* http://workspace.unpan.org/sites/Internet/Documents/UNPAN95735.pdf
[19] WSIS has created a matrix, linking WSIS action lines with SDGs. See https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_matrix_document.pdf
[20] *Supra* note 15.
[21] *See* operative paragraph 8 of the outcome document, A/70/L.33, http://workspace.unpan.org/sites/Internet/Documents/UNPAN95735.pdf
[22] *See* for instance, the Statement for Plenary session on International Peace and Security, Ministry of Foreign Affairs, Australia, http://foreignminister.gov.au/speeches/Pages/2015/jb_sp_150417.aspx?ministerid=4

in 2013 have recognized the applicability of existing international law in cyberspace.[23] The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) institutionalized the determination and consolidation of international law applicable to cyber warfare by introducing its Tallinn Manual Process in 2009. 'Tallinn 1.0'(The Tallinn Manual on the International Law Applicable to Cyber Warfare), a non-binding academic product, is the first tangible result of this process and covers issues of sovereignty, state responsibility, *jus ad bellum*, international humanitarian law and the law of neutrality in an effort to 'bring clarity to the complex legal issues surrounding cyber operations.'[24] However, the process has drawn criticism for its lack of global representation.

39. As the second iteration of the Tallinn Manual, dubbed 'Tallinn 2.0', works to expand its coverage to include peace-time international law, it too has expanded its engagement with the wider community. Tallinn 2.0 picks up where Tallinn 1.0 left off, and will set forth the experts' views on what international law applies to cyber activity that falls below the threshold of armed conflict or the use of force. Tallinn 2.0 has the potential to be even more influential than Tallinn 1.0 because it systematically will address activities that are far more prevalent in the cyber realm than uses of force or armed attacks. Tallinn Manual 2.0 draft includes sections on human rights, diplomatic law, the responsibility of international organizations, international telecommunications law, and peace operations. The Tallinn Manual 2.0 is on track to be completed and published in the second half of 2016.

40. To address the criticism that Tallinn process is devoid of global consultations, the NATO CCDCOE organized a meeting of International Group of Experts with legal advisers from European, North and Latin American, African, and Asian and Asia-Pacific states to gather national viewpoints and concerns to include in the decision-making process.[25] Many AALCO Member States including China, India, Japan, Pakistan, Republic of Korea, Sri Lanka and Thailand participated in the meeting.[26]

IV. Comments and Observations of the AALCO Secretariat

41. The recent discussions and deliberations in international forums on cyber governance makes it amply clear that the international community has gradually embraced the idea of a more equitable and transparent multi-stakeholder framework for regulating cyberspace. Currently, these discussions focus on finalization of the proposal for ICANN's oversight moving from the U.S. government to a multi-stakeholder group. This multi-stakeholder group, though envisaged to be independent from U.S. oversight, is expected to be

[23] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

[24] The Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013

[25] *35 States attend Tallinn Manual Consultations*, https://ccdcoe.org/35-states-attend-tallinn-manual-consultations.html

[26] The details of the consultation meeting are not available in the public domain.

dominated by the information technology industry mainly controlled by western enterprises.

42. It should also be noted that even though after transition, the numerous judicial, executive and legislative powers held by the U.S. government over ICANN as an American organization remain unchanged. Given these concerns, what is required is to get ICANN incorporated under international law, with host country immunities for an international organization. The AALCO Secretariat urges the Member States to actively participate in the IANA transition process to ensure the independence of ICANN and to ensure that the transition will result in a democratic institution which also pay heed to the concerns of the developing nations. Put simply, any new arrangement shall not only be multi-stakeholder, but also multilateral in nature as emphasized by some Member States of AALCO/

43. Further, the Secretariat welcomes the broader consultative process started by the NATO CCDCOE before the finalization of Tallinn Manual 2.0. The importance of this process cannot be understated as the laws applicable to transnational cyber attacks and transgressions falling below the level of cyber warfare are still unconsolidated and often open to disputes. The Secretariat encourages the Member States to include their comments on the process in their interventions so that they can be conveyed to the international group of legal experts in charge of the Tallinn Manual process.

Annex

SECRETARIAT'S DRAFT
AALCO/RES/DFT/55/S17
20 MAY 2016

INTERNATIONAL LAW IN CYBERSPACE

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

Having considered the Secretariat Document No. AALCO/55/HEADQUARTERS (NEW DELHI)/2016/SD/S17,

Noting with appreciation the introductory statement of the Deputy Secretary-General,

Also noting with appreciation the Special Study of the topic prepared by the AALCO Secretariat,

Welcoming the Summary Report of the Chairperson of the open-ended Working Group on International Law in Cyberspace,

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

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,

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

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

Noting with concern the use of cyberspace for military purposes and the escalation in various kinds of cyber attacks perpetrated by State and non-State actors,

Underlining 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 Working Group on International Law in Cyberspace to hold inter-sessional meetings, preferably in cooperation with Member States and relevant international organizations and other institutions, in pursuance of its mandate;

3. **Directs** the Secretariat to closely follow developments in international forums related to governance of cyberspace and cyber security; and

4. **Decides** to place this item on the provisional agenda of the Fifty-Sixth Annual Session.