AALCO/59/HONG KONG/2021/SD/S17

For Official Use Only

ASIAN-AFRICAN LEGAL CONSULTATIVE ORGANIZATION

INTERNATIONAL LAW IN CYBERSPACE

The AALCO Secretariat
29-C, Rizal Marg,
Diplomatic Enclave, Chanakyapuri,
New Delhi – 110 021
(INDIA)

INTERNATIONAL LAW IN CYBERSPACE

CONTENTS

I. Introduction

A. Background

1. The topic 'International Law in Cyberspace' was introduced as an agenda item to be deliberated at the Fifty-Third Annual Session of AALCO held in Tehran, Iran, in 2014, on the recommendation of the People's Republic of China. The agenda was subsequently deliberated as a substantive topic again in the following year in 2015, at the Fifty-Fourth Annual Session held in Beijing, China. The Resolution on the agenda item adopted in that 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, 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'.[1] It was further decided vide the said resolution that an 'Open-ended Working Group (OEWG) in International Law in Cyberspace would be established to further discuss on the issues identified above, through meetings or workshops to be cosponsored with Governments of the Member States or relevant international organizations'.[2]

2. Accordingly, the first OEWG on International Law in Cyberspace met during the Fifty-Fifth Annual Session in New Delhi, India in 2016. Prof. Huang Zhixiong was elected as the Rapporteur, and Mr. Hossein Panahi Azar as the Chairperson of the OEWG. The resolution adopted on the agenda item at the Fifty-Fifth Annual Session directed the Secretariat to '…closely follow developments in international forums related to governance of cyberspace and cyber security and continue its study on International Law in Cyberspace pursuant to the relevant resolution adopted in the Fifty-Fourth Annual Session…', and the OEWG '…to hold intersessional meetings… taking into account the need of AALCO Member States in combating cybercrime.'[3] The second OEWG on International Law in Cyberspace took place from 9-10 February, 2017, at the AALCO headquarters, New Delhi. The following topics, which were already identified by the Member States from the very start as being of utmost relevance, were discussed at the second OEWG, namely: a) Sovereignty in Cyberspace: Balancing Rights and Obligations, b) Law and Governance of Cyberspace, c) Cyber Warfare: Legal Implications, and d) Cybercrimes and International Law. The draft of the Special Study prepared by the Secretariat, containing broadly the same topics as above, was also discussed during the second OEWG.

3. At the Fifty-Sixth Annual Session in Nairobi, Kenya in 2017, the topic International Law in Cyberspace was once again taken up as a substantive agenda-item. The Secretariat's Special Study on International Law in Cyberspace was released therein. The resolution adopted during the session directed the Secretariat to '…closely follow developments in

[1] AALCO/RES/54/SP2, Beijing, 17 April, 2015.
[2] AALCO/RES/54/SP2, Beijing, 17 April, 2015.
[3] AALCO/RES/55/S17, New Delhi, 20 May 2016.

international forums related to governance of cyberspace and cyber security, and to organize OEWG meetings, as and when necessary', and the Rapporteur 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 OEWG'.[4]

4. The Report prepared by the Rapporteur of the OEWG on International Law in Cyberspace on the future plan of action of the OEWG, was firstly sent to all the Member States, through the AALCO Secretariat, for their comments and observations. Comments from a number of Member States were received by the Secretariat, and on the basis of that the Rapporteur prepared a revised report, which was also circulated to all the Member States. The revised report was thereafter discussed at the third OEWG on International Law in Cyberspace, which took place on the side-lines of the Fifty-Seventh Annual Session in Tokyo, Japan in 2018.

5. At the Fifty-Seventh Annual Session, the broad consensus reached as to the future plan of action of the OEWG was as follows: a) the OEWG continue to discuss the issue of international law in cyberspace with the aim to, *inter alia*, enhance cooperation in countering cybercrime, research on some key issues of international law in cyberspace, and identify areas for capacity building as appropriate; b) the Rapporteur prepare a report on the latest developments on international law in cyberspace; and on the special need of the Member States for international cooperation against cybercrime; c) the agenda item "International Law in Cyberspace" remains on the agenda of the Organization and the next Annual Session as well, and the OEWG continues its work on the subject matter; and d) the OEWG considers having at least one meeting before or during the next Annual Session to receive the views of the Member States and enhance further consultation on the item, subject to the availability of financial resources.

6. In preparation of the Rapporteur's Report on 'Special Need of the Member States for International Cooperation against Cybercrimes', as mandated by the Fifty-Seventh Annual Session, a questionnaire prepared by the Rapporteur was circulated among the Member States, to which responses from 11 Member States were received. The questionnaire, consisting of 38 questions, included four parts, namely: a) domestic law, b) international cooperation, c) capacity building and technical assistance, and d) public-private partnership. The fourth OEWG on International Law in Cyberspace was held from 2-4 September 2019 in Hangzhou, the People's Republic of China, chaired by H.E. Dr. Abbas BagherpourArdekani. The Rapporteur presented his Report on the outcome of the Member States' Response to the Questionnaire. The Chairconcluded 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 the AALCO Member States. The need to find common ground among the Member States was the most important aspect of the topic and could form the basis of the forthcoming Annual Session of AALCO. He further requested 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. Thereafter, challenging issues of international law in Cyberspace

[4] AALCO/RES/56/S17, Nairobi, 5 May 2017.

were discussed, namely: a) Application of the Principle of Non-Interference in Cyberspace; b) Data Sovereignty, Trans-border Data Flow, and Data Security; and c) Regulating Online Harmful Content. Lastly, the topic of 'Peaceful Use of Cyberspace' was discussed by the participants.

7. Further in this regard, the Secretary-General's proposal on 'Consensual Basic Principles of International Law Applicable in Cyberspace' (as mandated by the Fourth OEWG) had been drafted and circulated to the Member States. On the first draft comments were received from five Member States. Based on these comments and an internal review of the principles, the principles were revised. The revised draft of July, 2021, consists of carefully and elaborately drafted set of 14 principles, and an *Explanatory Note* to the same. On this revised draft comments have been received from three Member States so far.The revised draft and the comments received would be submitted to the Fifth OEWG Meeting on International Law in Cyberspace for further in-depth discussions and possible adoption.

8. At the Fifty-Eighth Annual Session, in Dar-es-Salaam, the United Republic of Tanzania, in October, 2019, the Member States expressed their views in general on the use of cyberspace, specifically focusing on topics such as principle of non-intervention in cyberspace, privacy issues, international law applicable to cyber-attacks, regulation of online content, a multilateral convention that may regulate activities within cyberspace, enhancement of cooperation in combating cyber-crimes, as well as the importance of a non-binding general document under the AALCO premises clarifying the consensual basic principles of international law applicable in cyberspace.

9. It must be noted that the Member States' Response to the Questionnaire made by the Rapporteur in preparation of his Report on 'Special Need of the Member States for International Cooperation against Cybercrimes', as well as the Secretary-General's 'Proposal of the Consensual Basic Principles of International Law Applicable in Cyberspace' and the comments received would be discussed at the Fifth Meeting of the OEWG on International Law in Cyberspace, which is to take place on the side-lines of the Fifty-Ninth Annual Session, in accordance with the above mandates. This brief is, therefore, limited in scope to the topics for General Meeting discussion at the Fifty-Ninth Annual Session.

B. Issues for Focused Deliberations at the Current Annual Session

1) Application of the Principle of Non-Interference in Cyberspace
2) Data Sovereignty, Trans-border Data Flow, and Data Security
3) Regulating Online Harmful Content
4) Peaceful Use of Cyberspace

II. Deliberations at the Fifty-Eighth Annual Session of AALCO (Dar-es-Salaam, the United Republic of Tanzania, 21-25 October 2019)

10. The Secretary-General of AALCO delivered the introductory statement on the subject. He explained in brief how AALCO had dealt with the topic 'International Law in

Cyberspace' since the time it was added as a substantive agenda item in 2014. He further mentioned that the discussions on International Law in Cyberspace under the Fourth General Meeting of the Fifty-Eighth Annual Session were taking place against the backdrop of the Fourth Meeting of the OEWG on International Law in Cyberspace concluded in Hangzhou, China from 2-4 September 2019. Thereafter, he congratulated Prof. Zhixiong Huang of Wuhan University Law School, the People's Republic of China, for his work as the Rapporteur of the OEWG on International Law in Cyberspace; as well as the People's Republic of China and each of the other Member States for taking an active interest in the topic. He invited the Rapporteur, Prof. Zhixiong Huang to make a presentation on his ongoing work, as well as Prof. Zakayo N. Lukumay to initiate and assist deliberations in his individual capacity as an expert on the topic.

11. The first speaker, Prof. Zhixiong Huang, Rapporteur of the OEWG on International Law in Cyberspace, firstly mentioned that he has presented a Report on how the Member States responded to the Questionnaire on Cybercrime prepared by him, at the Fourth Meeting of the OEWG on International Law in Cyberspace held in Hangzhou. He mentioned that his present statement was going to be an updated Report. He informed the Member States that the Questionnaire prepared by him was in furtherance of the mandate received at the Fifty-Seventh Annual Session in 2018, which was to 'prepare a report on the latest developments on international law in cyberspace and on the special need of the Member States for international cooperation against cybercrime'. Summarizing the replies received from the Member States wherein they clarified their special needs for international cooperation against cybercrimes, he mentioned that the responses broadly indicated the Member States' need for enhanced international cooperation in combating cybercrime and for strengthening capacity building and technical assistance in this regard. He further welcomed inputs from other Member States of AALCO so that he would be able to complete his Report on the special need of Member States for international cooperation against cybercrime, as per the above-stated mandate.

12. The next speaker, Prof. Zakayo N. Lukumay, Senior Lecturer and Acting Principal of the Law School of Tanzania, in his presentation broadly examined the applicability of international law principles to cyberspace, namely - international cooperation, sovereignty, jurisdiction and law of armed conflicts. After explaining the global and anonymous nature of cyberspace, he mentioned that the same has also made it possible for criminals to engage in a variety of criminal activities in cyberspace. He added that cyberspace has also become area of inter-State conflicts, as cyber-attacks are becoming more and more common. This has necessitated the creation a system of laws and regulations known as cyber laws, already in place to varying degrees in different nations, he mentioned. With regard to cybercrimes, he further mentioned that there is no agreement among nations as to what could constitute a common definition of cybercrime, for it to be outlawed. Therefore, in order to generally define activities that could constitute punishable cybercrimes, he proposed application of international law - through the adoption of binding international legal instruments - for the global nature of the Internet.

13. He proposed that a State may exercise extraterritorial jurisdiction pursuant to Article 19 of the ICCPR as the State has the right under international law to defend itself against any cyber-attack threatening national security, public order or the lawful rights and freedoms of others, including the rights of privacy and intellectual properties. He further proposed with

respect to cybercrime that as the offence has an international character, a country should invoke the universal jurisdiction theory which would require some consensus among countries. Regarding the Budapest Convention as an instrument for forging international cooperation for fighting cybercrimes, he stated that it may not be an appropriate instrument to resolve all issues as it depends on the goodwill of the country you seek cooperation from. The Convention is also short on giving States the necessary tools to fight this type of crime, he mentioned.

14. On the issue of cyberterrorism, he proposed the use of the 1988 Rome Convention for the Suppression of Unlawful acts against the Safety of Maritime Navigation, which can also be interpreted to cover cyber-activities. On the question of international law applicable to cyber-war, he discussed various issues attached to the application of Articles 2 (4) and 51 of the UN Charter. In conclusion, he stated that in order to resolve issues relating to cybercrimes there is a need for an international legal binding instrument under the auspices of the United Nations.

15. The **Delegate from the Republic of Kenya**, while appreciating the unique nature of cyberspace that presents significant opportunities for the global community at large, conceded to the immense challenges that have emerged, and acknowledged the urgent need to address those challenges. In this regard, he appreciated the ongoing work in AALCO's OEWG on International Law in Cyberspace. In particular, he acknowledged the emerging legal issues surrounding misuse of computers and cyberspace in general; and the need for an international legal framework, in addition to existing regional frameworks, to enhance cooperation in combating cybercrime. He further explained in brief the domestic legal framework in Kenya to address the threat to cybersecurity under 'The Misuse of the Computer and Cybercrimes Act, 2018'. He further spoke about the Kenya Information and Communications Act, 2015 that has gone a long way in strengthening the multi-agency collaboration framework, among other key facets, that support national cyber security resilience. In conclusion, he offered assurance that Kenya is in the process of preparing detailed responses to the questionnaire that is to be submitted to the AALCO Secretariat.

16. The **Delegate of the United Republic of Tanzania** firstly noted that cyberspace ought not to be a lawless area, and that cyberspace is in fact subject to the principles of sovereignty and jurisdiction as well as prohibitions on intervention in the affairs of other States and the use of force. Further, for the international regulation of cyberspace he recommended the following: a) there should be an international legally binding instrument to regulate cyberspace. Moreover, there is a need to establish clarity on the role of international law in cyberspace since some States have begun disseminating their own interpretations of international law with regard to cyberspace; b) there is a need to determine whether existing law is sufficient or satisfactory to provide sufficient guidance and guarantees for States' inter-relations within cyberspace; c) there is a need to classify cyber-attacks that qualify as violations of international law; d) will of major cyber powers to discuss red lines for offensive cyber activity needs to be addressed; e) application of international law to cyberspace needs to be clear with respect to humanitarian costs of cyber-attacks especially when some organizations use cyberspace for communications and logistics that have been subject to cyber-attacks; and f) there must be multilateral responses to existing emerging threats in cyberspace.

17. The **Delegate of the Federal Democratic Republic of Nepal** firstly expressed appreciation for the OEWG on International Law in Cyberspace for its contribution to the development of international law of cyberspace. He expressed that international law has now moved from whether international law applies to cyberspace, to how international law applies in cyberspace, which in turn needs international consensus. In this regard he stated that a non-binding general document under the AALCO premises clarifying the consensual basic principles of international law applicable in cyberspace would be vital. He mentioned that in order to address the challenges of cyber security and issues of cyberspace, the Government of Nepal has endorsed a bill on Information and Technology to the House of Representatives. He further stated that since cyber security is not a mere domestic deal, special measures have to be established to address inclusion and cooperation among the Member States to enhance cooperation in capacity building and set uniform standards for combating cybercrime. In this regard he urged AALCO to take initiation in development of appropriate and effective rules of international law to combat cybercrimes and of an international regime that assists the international community in building a robust mechanism and modality, balancing between the State domain and public domain vis-à-vis development of a secured and inclusive cyberspace. In conclusion he notified that Nepal is under process of consultation with responsible authorities to contribute to the Rapporteur's Report on "Special Need of the Member States for International Cooperation against Cybercrime."

18. The **Delegate of the Republic of India** firstly acknowledged cyberspace as a complex domain where traditional concepts of sovereignty, jurisdiction and privacy are constantly challenged. He stated that in this regard it is imperative for States to understand and implement important norms already agreed in the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UNGGEs). He further noted that there is a need to develop better understanding of applicability of international law in cyberspace. Commitments of States under the UN Charter and other international law would apply to its behaviour in cyberspace.

19. However, the novel character of cyberspace and the vulnerability of cyber infrastructure have led to questions whether existing international law can provide sufficient answers to the emerging concerns in cyberspace, for example, working of the UNGGE reports so far do not clearly acknowledge that International Humanitarian Law (IHL) applies to State actions in cyberspace, he noted. He further stated that the International Community has to agree on common definitions of cyber sovereignty, jurisdiction, weapon conflict, crime, deterrence, attacks, etc. He informed the session that India participated in the discussions of fifth UNGGE leading to adoption of two resolutions in the UN First Committee of the General Assembly in November 2018, and in the first substantive meeting of OEWG on September 9-13, 2019 in New York, and that it endorses the need to have a common understanding on how international law is applicable to State which is possible under UN and other multilateral forums. The development and implementation of cybersecurity laws, policies and practices should be consistent with international law including international human rights law, he noted. In conclusion, he stated that deliberations on the above issues at AALCO, thus, should consider the work on the topic that is being conducted within the auspices of the UN, with a view to avoiding duplication of work.

20. The **Delegate of the Republic of Korea** firstly noted that Information and Communications Technologies (ICTs) along with bringing in boundless opportunities, and

unprecedented economic and social benefits, have also at the same time, brought about new security threats, namely cyber-attacks. He noted that cyber-security requires international cooperation, or even, multilateralism. Therefore, he stated that mutual cooperation, assistance, and information sharing is required, based upon the following critical elements, namely: a) the discussions at AALCO have the potential to further deepen States' understanding of the current landscape of the normative framework for cyberspace and the challenges ahead; and b) practical measures designed for capacity building at the national, regional and global levels play a critical role in enhancing transparency and resilience in cyberspace. He informed that Korea is also actively participating in the discussions on cyberspace norms in the UN GGE (Group of Governmental Experts) setting as well as holding bilateral cyber policy consultations with a dozen countries. In conclusion, he added that the Republic of Korea has already submitted its answers to the questionnaire of the AALCO OEWG on International Law in Cyberspace, which he is hopeful would deepen the understanding of cyberspace actors about cyberspace issues and promote cooperation among States.

21. The **Delegate of the Islamic Republic of Iran** firstly appreciated the work of AALCO and the Rapporteur of the OEWG on Cyberspace on the topic, and especially for preparation of the questionnaire on international cooperation in dealing with cybercrimes. He stated that the Islamic Republic of Iran has been keenly following the work of AALCO and the OEWG on International Law in Cyberspace on this topic, and that it considers the OEWG to be a convenient platform for the Member States to exchange ideas in a legal context and to contribute appropriate development of international law on cybercrime. He mentioned that the Fourth OEWG Meeting that took place at Hangzhou, China, discussed some very pertinent issues such as international cooperation in combating cybercrimes, application of the principle of non-intervention and also issues related to data sovereignty, wherein Iran took an active part.

22. With regard to combating cyber-crimes he informed that Iran continues to participate in the relevant discussions within the context of the United Nations so as to come up with a universally negotiated and adopted instrument on combating cybercrime. He further informed that domestically the Islamic Republic of Iran has taken some important steps including ratification of Cybercrime Act (2009), Electronic Commerce Act (2003), the Law on Publicizing and Access to Data (LPAD) (2010) which provided legal ground in Cyberspace. With regard to executive measure in fighting cybercrimes, the Government of the Islamic Republic of Iran established Cyber Police in 2011 as an active organ in combating cybercrimes, he notified. He further informed that the Islamic Republic of Iran has also signed agreements and Memorandums of Understanding with different countries; particularly in the regions of western and central Asia.

23. With regard to the principle of non-intervention, he stated 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 needs further work and deliberation. In conclusion, while appreciating the work of the Secretary-General in drafting the consensual basic principles of international law applicable in cyberspace, he mentioned that the Islamic Republic of Iran would present its comments on this draft in due course.

24. The **Delegate of the People's Republic of China** firstly advocated the principles of peace, sovereignty, shared governance and shared benefits in international exchange and cooperation in cyberspace. He stated that the real challenge lies today in determining how international law principles apply in cyberspace. He mentioned that China supports the formulation of universally accepted international rules in cyberspace through multilateral and equitable, democratic negotiations under the United Nations, in which respect it is expected that the new Group of Governmental Experts and an Open-ended Working Group under the aegis of the UN would yield positive results.

25. Regarding the issue of combating cybercrimes, he stated that due to the differences in law and practices amongst States, the challenges in combating cybercrime cannot be solved by a few regional conventions, including the Budapest Convention concluded 18 years ago - and that the only effective solution is to collectively develop an international legal instrument that is negotiated by all States, and is open to all States. He further mentioned that Russia, China and a number of other States co-sponsored a draft UNGA resolution in New York, requesting the General Assembly to establish an open-ended intergovernmental committee to elaborate a comprehensive international convention on combating cybercrime, which, if adopted, would provide an important platform for developing countries to participate in international rules making process for combating cybercrime.

26. Regarding the issue of cyberwarfare, he stated that China firmly opposes cyber warfare or cyber arms race, and urges all the AALCO Member States to support the peaceful use of cyberspace, as given the 'digital gap' between developing and developed countries, developing countries in general will be in a disadvantaged position in the discussion and development of such rules, and that it will be difficult to ensure the rules are fair and equitable. Next, he hailed the AALCO OEWG on International Law in Cyberspace as an important platform that covered a broad range of new and important issues in international law in cyberspace, including combating cybercrime, regulating online harmful content, and issues relating to trans-border data flow - which could possibly assist the Member States to prepare themselves for the possible international rules-making processes under the UN.

27. He further commended the consensus to explore the drafting of a non-binding general document clarifying the consensual basic principles of international law applicable in cyberspace as an important outcome of the OEWG Meeting. Appreciating the draft principles prepared by the Secretary-General, he noted that the principles concerning trans-border data flow and the regulation of online harmful content are missing in the Secretary-General's draft, hoping that they would be included in the next iteration of the draft principles. He also expressed pleasure that China could host the 4th meeting of the OEWG in September 2019. In conclusion, he urged all the AALCO Member States to actively participate in the discussion of the OEWG, and thereby enhance their capacity for cyberspace governance and rule-making.

28. The **Delegate of the Republic of Indonesia** firstly touched upon various regulatory steps taken by the Government of Indonesia to promote peaceful use of, and economic growth through, cyberspace, including Law Number 11 of 2008 on the Electronic Information and Transaction, which then was amended by Law Number 19 of 2016; Government Regulation Number 71 of 2019 on the Use of System and Electronic Transaction; and new regulations that are being prepared namely, the bill on Cyber Security

and Resilience, the bill on Personal Data Protection, and the National Strategy on Cyber Security. A number of regulations to combat conventional crimes using cyberspace have also been prepared, for instance drugs-related crimes, human rights violations (especially those involving children, child discrimination, exploitation, and violence), as well as counter terrorism and violent extremism, including the National Action Plan on Countering Extremism that Leads to Terrorism, he added.

29. He stated that Indonesia agrees in principle for the adoption of the 11 Cyber Norms on Responsible State Behaviour in line with the 2015 UN GGE Report. He further underlined the following guidelines for cyberspace: a) global principles and norms to develop global architecture in cyberspace in various forums, including both the UN and AALCO through multi-stakeholder approach to develop tolerant and inclusive cyberspace; b) developing open, free, and safe cyberspace for peaceful purposes with respect to State sovereignty and human rights through inclusive participation; and c) the use of diplomatic solutions and the avoidance of military force in resolving cyberspace conflicts. He further appreciated the work of the Fourth OEWG on International Law in Cyberspace, and especially the outcome of consensual basic principles of International Law Applicable in Cyberspace. He mentioned that the Republic of Indonesia fundamentally agreed with principles (a) to (g) of the Secretary-General's Draft of the 'Consensual Basic Principles of International Law in Cyberspace', while noting that principle (h) needed further discussions as it is essentially under the realm of military and ought to be discussed through forums such as defence dialogue etc.

30. He further encouraged the AALCO Secretariat for the following: a) to establish AALCO's point of contact directory consisting high and working levels. The point of contact shall coordinate and confirm when cyber incidents occur; b) to support social media companies to assist governments of the AALCO Member States in filtering the spread of negative contents on terrorism, pornography (including child online protection on discrimination, exploitation, and violence), and other cybercrime related matters; and c) to enhance public-private partnership through building collaboration to prevent the misuse of the Internet.

31. The **Delegate of the Socialist Republic of Viet Nam** firstly expressed his concerns on the application of international law in cyberspace, as cyber-security has increasingly become a global issue, posing unforeseeable security risks. He stated that in the past Viet Nam has frequently suffered from issues of 'fake news' and other forms of cyber-attacks, threatening the national security and causing loss to State entities and nationals. The lack of a universally accepted set of norms to govern activities in the cyberspace, including application of established principles of international law in cyberspace calls for immediate action on the part of States. With regard to national laws to enhance cyber-security, he mentioned that the following law has been enacted within Viet Nam, namely, the Comprehensive Law on Cyber-security enacted in June 2018, and that a Governmental Decree detailing the implementation of the Law was now being built to substantially govern the entire cyber-security of the nation.

32. Regarding international cooperation on cybersecurity, he mentioned that without such cooperation a common understanding of how international law applies in cyberspace could hardly be obtained. In this regard, he stated that even though Viet Nam has yet not become a party to any international convention in this regard, it is gradually improving its national legal

framework in this area with a view to ensuring its compatibility with the current relevant international norms and standards, including exchanging views with other ASEAN members on combating cybercrimes, with the understanding that international law, especially the principles set forth by the UN Charter, shall be applicable to cyberspace.

33. He further added in this respect that as cyberspace is an evolving phenomenon, it should draw lessons from other domains such as outer-space and the law of the sea. While appreciating AALCO acting as a platform for effective regional cooperation for combatting cyber-crimes, he especially noted the useful work done by the Rapporteur of the OEWG on International Law in Cyberspace, including the contributions made by various Member States. He further appreciated the work done by the Secretary-General in his draft on 'Consensual Basic Principles of International Law in Cyberspace', while also noting that the topic requires further study and should not be rushed for the purpose of adopting an outcome document. In conclusion, he mentioned that even though the Member States could hardly reach an agreement during the Fourth OEWG meeting, exchanging views is the only way for States to deepen mutual understanding and to come up with resolutions.

34. Thereafter, the Vice-President opened the floor for comments by observer delegations.

35. The **Delegate of the International Committee of the Red Cross (ICRC)** made his statement on limits that international humanitarian law, or IHL, imposes on the use of cyber operations during armed conflicts. He stated that as cyber operations are being used in ongoing armed conflicts, ICRC is concerned with their potential human cost, and that in this regard it is critical that States affirm that IHL limits the use of cyber operations during armed conflict and protect civilians and civilian objects, as it does with any other means and methods of warfare. He also stressed at the same time that the application of IHL does *not* mean to legitimize conflicts, neither in the traditional domains of warfare nor in cyberspace. This is governed by the UN Charter and relevant customary international law. Therefore, IHL provides an additional layer of protection and a sense of humanity in the midst of such suffering, he noted.

36. In this regard, he welcomed the Secretary-General's draft on 'Consensual Basic Principles on International Law Applicable in Cyberspace' as a tangible outcome of the Fourth OEWG on International Law in Cyberspace, and especially principle 2(h), which is the provision addressing the military use of cyberspace and aimed at ensuring respect for IHL. By adopting a principle to this effect, AALCO would substantially contribute to progressing the international conversation on the issue, he noted. He encouraged the AALCO Member States to continue to study how IHL restricts the use of cyber operations during armed conflicts. In conclusion, he noted that while it is true that the development of military cyber capabilities and their use during armed conflict cannot occur in a legal void and is constrained by existing international law, including IHL; at the same time there is no doubt that as with the development of any new method of warfare, States may agree upon further rules to prohibit or limit specific military cyber capabilities or operations for a range of reasons, including humanitarian reasons, which should build upon and strengthen existing law.

37. The **Delegate of the Russian Federation** firstly stated that the application of international law is not that simple as it may so appear as since the adoption of the latest

report of the Group of Governmental Experts in 2015 the discussion has not progressed significantly. He stated that one of the primary reasons for the same is the divergence in the views of States regarding the nature of the use of this domain. One group to which Russia belongs tries to develop legal aspects of the peaceful use of ICTs including practical issues of protecting the sovereign equality of States, non-interference and cooperation, while on the other hand the other group of States put on top analysis of military use of ICTs including the applicability of Article 51 of the UN Charter and the right of self-defence, he noted.

38. He further noted that the latter view intends to secure the right to apply countermeasures in response to cyber-attacks while avoiding or directly refusing to discuss the problem of establishing relationship between the attack and the corresponding State as well as the problem of establishing standards of proof for such a connection and the damage caused. However, Russia considers the question of the standard of proof and attribution of the computer attack to the State in order to establish its international legal responsibility should precede any light weight generalizing conclusions and whether any countermeasures can be taken in response even more so in light of Article 51 of the UN Charter, he stated. Recognizing certain types of use of ICT as an armed attack gives right to reciprocal use of force can plunge the world into chaos, and unpredictable consequences, he added. In the same context, he noted that the general applicability of IHL is, likewise, a tricky question. He stated that the practical application of the principle of peaceful cooperation in the field of ICT is the key principle of the application of international law in cyberspace, which is supported by various UN General Assembly Resolutions. Regionalism in this matter may turn out to be dangerous, he further noted.

39. Regarding the issue of cybercrimes, he stated that States regardless of their level of development cannot effectively deal with cybercrimes without proper international cooperation, and that in this regard there is indeed a need for an international binding instrument under the auspices of the United Nations. This instrument should be based on the principles of sovereign equality and non-interference, with the following objectives: a) to promote and strengthen measures to prevent crimes and other illegal acts; b) to ensure the prosecution of such acts, facilitating the identification and investigation of such acts; and c) to increase efficiency of international cooperation including training and technical assistance; he noted. In conclusion, he stated that in this regard Russia, China and a number of other States drafted the UN General Assembly resolution entitled ‘Countering the use of ICTS from criminal purposes’ which on the one hand makes it possible to build on the discussions of this issue held in the UN General Assembly this year, and on the other hand creates a negotiating platform which may be used in the long term.

40. After the statements of observer delegates, the **Delegate of the Sultanate of Oman**asked the floor. He firstly expressed appreciation for and agreed with the conclusions of the OEWG on International Law in Cyberspace at its fourth meeting held in Hangzhou, China from 2-4 September 2019 on the importance of cooperation among the Member States in the field of combating cybercrime, as well as the draft prepared by the Secretary-General on the applicable principles of international law on cyberspace. He stated that as cyber threats severely affect sovereignty, security, economic and social stability of States, they have no options but to cooperate with each other, to formulate the legal regulation governing transit, content and harmful use of cyberspace. In this regard, he lauded the work of the OEWG on International Law in Cyberspace of AALCO that acted as the stepping stone which the

Member States can build upon in order to adopt a unified, clear-cut position that can be put forward in other international forums.

III. General Discussions and Recent Developments

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

41. Sovereignty in the contemporary public international law denotes the basic international legal status of a State that is not subject, within its territorial jurisdiction, to the governmental, executive, legislative, or judicial jurisdiction of a foreign State or to foreign law other than the public international law.[5]

42. Given its unique characteristics – commonly described as a great 'no place' or a domain without real boundaries that transcends physical space – the application of sovereignty in cyberspace, however, is far from being straightforward. While actions in the cyber domain seem to take place outside the physical boundaries of any State in a virtual world, their effects nevertheless have real world implications that are quite often felt inside States. Moreover, ICT infrastructure is owned by the government or corporations, which is connected to the national Internet grid. Further, a nation's prerogative to control events within its territory entails the power to regulate the local effects of extraterritorial acts. So while it is true that the unique architecture of cyberspace makes it challenging for the States to exercise their sovereignty, the technical problems involved do not and cannot prevent a State from exercising its sovereignty. An AALCO Member State summarized it perfectly in its statement at the Fifty-Fourth Annual Session of AALCO – 'The elusive feature of this type of jurisdiction requires that it be controlled by all States'.[6]

43. The UNGGE in both the 2013[7] and 2015 editions declared that international law, and in particular the UN Charter, were applicable to cyberspace. However, the questions on how it applies continues to remain unsolved. Tallinn Manual 1.0 and 2.0 have also affirmed the application of international law into cyberspace. Rule 1 and 2 of the Tallinn Manual 1.0 explain the legal basis for such exercise of jurisdiction.[8] Rule 1 clearly states that a State may exercise control over cyber infrastructure and activities located within its sovereign territory, which includes land territory, internal waters, territorial sea, archipelagic waters and national airspace. This right is the natural extension of sovereignty the State enjoys over its territory. Rule 2 elaborates that without prejudice to applicable international obligations, a State may exercise its jurisdiction: a) over persons engaged in cyber-activities on its territory, b) over

[5] H. Steinberger, *Sovereignty*, (Max Planck Institute for Comparative Public Law and International Law, Encyclopedia for Public International Law, Vol. 10 (1987)), p. 414.
[6] Statement by the Islamic Republic of Iran, Agenda Item: International Law in Cyberspace, Fifty-Fourth Annual session of AALCO, Beijing, 2015.
[7] The UNGGE in its 2013 report declares that 'State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory'. See 'Developments in the field of information and telecommunications in the context of international security', Report of the Secretary-General, A/68/156, 2013.
[8] See *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge University Press, 2013), pp. 25-30.

cyber infrastructure located on its territory, and c) extraterritorially, in accordance with international law.

44. The magnitude and frequency of cyber-attacks have continuously grown since the inception of the World Wide Web. Starting from the nuisance of individual hackers in the early years, to high intensity cyber aggression against States – Governments have responded to these attacks with the creation of various military and governmental cyber-security agencies, and with legislations directly addressing the critical importance of cyberspace security.

45. The United Nations Charter, by prohibiting the threat or use of force under Article 2(4) as the main pillar of *jus ad bellum* imposes fundamental limitations on cyber warfare. The International Court of Justice (ICJ) has opined that Articles 2(4) and 51 of the UN Charter regarding the prohibition on threat or use of force and self-defence, respectively, apply to 'any use of force, regardless of the weapons employed'.[9] IHL imposes limitations on the use of cyber operations during armed conflicts, with the ICRC maintaining that IHL limits the use of cyber operations during armed conflict and protect civilians and civilian objects, like it does with any other means and methods of warfare, and that its implication is not to legitimize conflicts. Some States, however, do maintain that acceptance of the applicability of Article 51 of the UN Charter to cyberspace amounts to its militarization and negates the broader ideal of peaceful use of cyberspace. The broad principle of non-intervention under international law provides limited guidance in the realm of cyberspace because the vast majority of cyber operations do not trigger the kinetic thresholds of use of force, and as such do not fit squarely within the traditionally recognized elements of the non-intervention rule.

46. Intervention is traditionally understood as coercive interference in matters that fall within a State's sovereign affairs such as the choice of political, economic, social and cultural system and the formulation of foreign policy. Cyberspace provides a facilitative environment where intervention can take place, diversifies its means and methods but also enhances its scalability, reach and effects. In the recent past, the use of cyberspace for electoral interference has increased manifold and has had tremendous and far-reaching consequences. Such interference mainly consists of attacks on electoral infrastructure and operations to manipulate voting behaviour. International law commentators struggled to qualify such operations. Although the majority placed them within the framework of the principle of non-intervention, they concluded that they do not satisfy its conditions and in particular that of coercion.[10] Some authors, however, maintain that electoral cyber interference can violate the non-intervention principle by arguing that voter-manipulation may amount to 'coercion'.[11]

47. On six occasions since 2003, UNGGEs have been established to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including the GGE of 2019-21. Through their three consensus reports (2010, 2013 and 2015), which are cumulative in nature, these Groups have reaffirmed that

[9] Nuclear Weapons Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 ICJ 226 (July 8), para. 39.
[10] See for example, Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', Cornell University Law School, 2017.
[11] Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace', *EJIL:TALK!*, (2019),

international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability in the ICT environment. They also recommended 11 voluntary non-binding norms of responsible State behaviour and recognized that additional norms could be developed over time. Furthermore, specific confidence-building, capacity-building and cooperation measures were recommended. In General Assembly resolution 70/237, Member States agreed by consensus to be guided in their use of ICTs by the 2015 GGE report, thereby consolidating an initial framework for responsible State behaviour in the use of ICTs.

48. The fifth UNGGE tasked with developing a 'common understanding' of how States should behave in cyberspace failed to reach a conclusion in 2017 with several States not agreeing to the final draft report. The 2016-17 UNGGE had made measurable progress in clarifying certain norms of behaviour for State and non-State actors; however, States could not agree on draft paragraph 34, detailing how international law applies to the use of ICTs.

49. In 2018, another UN-mandated working group – the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) – was established in parallel with the GGEs, involving 'all interested States'. In accordance with its mandate the OEWG has discussed existing and potential threats in the sphere of information security and possible cooperative measures to address them; further development of rules, norms and principles of responsible behaviour of States; how international law applies to the use of ICTs by States, confidence-building measures, and the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations. The OEWG's mandate was renewed for 2021/2025 in December 2020. It adopted its final report by consensus in March 2021.[12] The final report was unanimously adopted by 68 participating States, becoming the first report on cybersecurity of this scale adopted with direct governmental participation.

50. The report reaffirms the previous GGE statement that international law, including the UN Charter, is applicable to cyberspace. The OEWG also expressly recognizes dispute settlement mechanisms provided in the UN Charter, encouraging States to "seek the settlement of disputes by peaceful means such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements, or other peaceful means of their own choice". The report concludes that the most effective way to reach common ground on the concrete application of international law to the ICT environment is through regular exchange of views and practices, and identification of specific international law issues that require in depth conversations, under the auspices of the UN and the Secretary-General.[13] Overall, the report refrains from specifying concrete international law branches that might apply, the prospect of which had raised high expectations.

51. In GA resolution 73/266, the Secretary-General was requested to establish a GGE on Advancing responsible State behaviour in cyberspace in the context of international security. The GGE held its first meeting in 2019 and submitted its final report to the General Assembly in 2021. The group is comprised of 25 Members and its Chair will hold two informal

[12] 'Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Substantive Report', United Nations General Assembly, A/AC.290/2021/CRP.2, 10 March 2021.
[13] *Ibid.*

consultations with all UN Member States in between its sessions. The mandate also includes consultations on the subject to be held with regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations.

52. During the discussions at the 2019 GGE the elements on international law in the 2013 and 2015 reports, notably that international law, and in particular the Charter of the United Nations, is applicable to State uses of ICTs, was re-emphasized, although questions on how it applies remained. Further, it was stated that the applicability of international humanitarian law to cyber operations during armed conflict does not encourage the militarization of cyberspace or legitimize cyber warfare, just as it does not legitimize any other form of warfare. Further, regarding the applicability of IHL, its applicability to the use of new weapons, means and methods of warfare during armed conflicts, including those relying on ICTs was noted.[14]

53. The GGE concluded its work by adopting a consensus report on 28 May 2021.[15] Given the failure of the last GGE, including the aftermath of severe hostile cyber operations against GGE members, the Working Group's efforts to reach consensus and compromise on key issues represent important progress. Many aspects of the Report overlapped with those of the OEWG Report, given the similarity in their respective mandates, perhaps the most substantive step forward for the GGE is its acknowledgment that IHL applies to cyber operations during an armed conflict, including by evoking the fundamental principles of humanity, necessity, proportionality, and distinction. As disagreement still remains on concrete interpretation of IHL principles, the GGE recognized the need for further dialogue on qualification of key terms in the cyber context. Unlike the OEWG report, the GGE's 2021 report expands on principles of international law that might be relevant in cyberspace. Building on the 2015 report, which mentions State commitment to sovereign equality, the GGE's 2021 report includes a prohibition of the threat or use of force against the territorial integrity or political independence of another State, respect for human rights and fundamental freedoms, and non-intervention in the internal affairs of other States. Like the OEWG report, however, it underscores the vulnerability of critical infrastructure in the face of hostile cyberoperations.[16]

54. The GGE Report further develops means of compliance with voluntary, non-binding norms of responsible State behaviour agreed upon in 2015. Like the OEWG, it stresses the importance of international cooperation, and the value of capacity building measures. Overall, the GGE emerged as an inclusive process on the application of international law to cyberspace and demonstrated significant progress from its previous rounds, especially regarding the application of IHL to cyberspace; although a number of issues still deserve close attention. Issues such as sovereignty, due diligence, interreference, the meaning of *attack* in the cyber realm, the scope of State accountability, and countermeasures remains

[14] Chair's Summary, Informal Consultative Meeting of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 5-6 December 2019, available at: https://www.un.org/disarmament/group-of-governmental-experts/.
[15] 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', Advance Copy, 28 May 2021.
[16] *Ibid.*

unsettled, as do calls for a transparent mechanism to assess and track the progress of norm implementation.[17]

2) Data Sovereignty, Trans-border Data Flow, and Data Security

55. Today we are living in a 'Digital Age' where data is more valuable than ever. Just as the global manufacturing industry half a century ago learned to adapt to an age of automation, companies today are learning to adapt to an age of digitization. In recent years, proponents of data globalization have been at loggerheads with the proponents of data localization. The former ones have been promoting free and open flow of data across borders, while the latter of these have been adopting measures curtailing cross-border data flow citing privacy and security concerns.

56. 'Data sovereignty' is the idea of data being subject to the laws and governance structures of the country where it is being collected, as against the country where it is stored or processed, or where the company storing the data is incorporated. Stealing and surreptitiously transmitting users' data in an unauthorized manner to servers that are located outside the country where the data originated, and the subsequent compilation, mining and profiling of these data by elements hostile to the national security of the said State, may have severe consequences for the sovereignty and integrity of such State. Many States today, therefore, are of the view that data are a sovereign asset, and that government restrictions on data flows would allow States to be able to use 'personal, community and public data' generated in the country towards the welfare and development of its people. However, there is also the pro-privacy argument that treating data as a sovereign asset takes away from individual rights over data, and trades them away for a higher GDP figure and greater State control. There are also alternative conceptions that advocate a middle path of sovereignty that aims to bring back control and autonomy to people. These conceptions provide a framework within which there is a possibility to articulate questions about the agency of the individual, and of collective interest.

57. Data protection laws date back to the 1970s, reflecting concerns about the emergence of computer and communication technologies, with their ability to process remotely large volumes of data. Lawmakers have increasingly recognized the Internet as both a 'critical national infrastructure', over which an increasing proportion of daily economic and social activities is carried out, and as a source of vulnerability and threat. Addressing this duality and putting in place adequate data security measures is, therefore, a core component of the legal and policy response. The role of data security is fundamental. Whether physical, logical or organizational, security measures should protect against deliberate acts of misuse, as well as the accidental loss or destruction of data.

58. With regard to the issue of data sovereignty, furthermore, determining jurisdiction has become a very prominent issue in data protection regulation, partly due to the widespread flow of data across borders, and partly to the lack of a single global agreement on data protection (and the consequent fragmentation of regulation). In the absence of an

[17] *Ibid.*

international agreement, jurisdiction law is complex. Establishing sovereignty is an especially important concern amid legal and policy constraints when data and resources are virtualized and widely distributed. The exponential growth of electronic data has led private organizations and governmental agencies with limited storage and IT resources to outsource data storage to cloud-based service providers. Actually, verifying that cloud storage service providers are meeting their contractual geographic obligations, however, is a challenging problem, and one that has emerged as a critical issue. Therefore, there is the need for developing new algorithms for establishing the integrity, authenticity, and geographical location of data stored in the cloud.

59. The international transfer of personal data has resulted in economic growth and efficiencies that have had a positive impact around the world, while at the same time subjecting the privacy of individuals to new and increased risks. While the potential need to control cross-border flows of data for privacy purposes is clear, the application of such controls in an increasingly interconnected world is very challenging. ICT developments, such as cloud services, are making things even more complex, with processing entities not necessarily aware about where the data are located. Although the answer may eventually be a technological one, increased harmonization of laws and regimes would greatly reduce the likelihood of friction over cross-border data flows. The evolution of a new legal regime with particular rights and responsibilities relating to trans-border data flows is happening at a time when the opportunities for abuse of processed or stored data have increased considerably. The need for harmonized governing principles in the treatment of data crossing national boundaries has become compelling.

60. Notwithstanding the current global approach to the regulation of trans-border data flows, States do not always share identical interests. The pattern of trans-border data flows between developed and developing countries differ; processed data flow to developing countries and raw data flow out to developed countries. Thus, the call for regulating trans-border data flows generally pits developed States - States that benefit most from trans-border data flows - against developing States. The issue that arises is how to control or regulate the flow of personal data across national boundaries in an orderly manner that would not put the data privacy rights to undue or unacceptable risks. It has therefore become imperative to adopt a global approach to resolve these problems. There does not exist a truly global convention or treaty dealing specifically with data privacy - there are treaties that have so far engendered international cooperation and harmonisation, albeit at bilateral and regional levels.

61. Data security has come to occupy an important place in the current discussions at the international legal forums. First and foremost, the UN has had a long history of promoting the right to privacy through its Human Rights treaties, particularly through Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). It has strengthened its role in privacy protection through two high profile measures – one, publication of a statement on Digital Rights; and second, by the appointment of a Special Rapporteur on the right to privacy. In 2013 the UN adopted resolution 68/167, which expressed deep concern over the negative impact that surveillance and interception of communications may have on human rights, while affirming that the rights held by people offline must also be protected online, and it

called upon all States to respect and protect the right to privacy in digital communication.[18] The resolution was followed by a detailed report in 2014 entitled, 'The Study of the High Commissioner for Human Rights on the Right to Privacy in the Digital Age', which concluded that *'practices in many States have ... revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy*'.[19]

62. Every year the UN Special Rapporteur on the right to privacy presents an annual report to the Human Rights Council and the UN General Assembly. In the 2020 Report of the Special Rapporteur of the Human Rights Council on the right to privacy submitted to the UN General Assembly, the Rapporteur examined two particular aspects of the impact of COVID-19 on the right to privacy: data protection and surveillance. The use of information and technology is not new in managing public health emergencies. The Report, however, concerned itself with the privacy-invasive nature of the contact tracing tools increasingly used by public health entities to trace the spread of communicable diseases. That is to say, it is a complicated scenario when surveillance apparatus traditionally employed for State security purposes are proposed or hurriedly deployed for a public health purpose such as combating COVID-19. The Rapporteur noted that where a State has a law that provides for extraordinary powers, and where any measures deployed when exercising such powers seem to be privacy-invasive, including any form of surveillance (e.g., geolocation, proximity monitoring, malware, telephone tapping, profiling), they should require oversight *ex ante* and *ex post* to prove that they are necessary and proportionate to the pursued objective. In that way, it would be guaranteed that only the appropriate surveillance method is carried out by the appropriate people, for the appropriate purpose and for the appropriate length of time.[20]

63. The Council of Europe Data Protection Convention of 1981 (usually referred to as Convention 108 or the CoE Convention) is the most prominent binding international agreement on data protection. Although this Convention was established by the Council of Europe, its membership is open to any country, and several non-European countries have signed the Convention. The OECD 1980 Guidelines on the Protection of Privacy and Trans border Flows of Personal Data (revised in 2013) were developed by OECD member states in consultation with a broad group of stakeholders. The real impact of the OECD Guidelines is their influence on the content of privacy laws around the world – well beyond the OECD's member base. The Guidelines contain eight privacy principles that form the backbone of the principles included in most national privacy laws. There is also the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2005), and the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection within ECOWAS 2010, which are quite successful at the regional level.

64. With regard to trade implications of data protection, itis relevant to note that Article XIV (c) (ii) of the WTO's General Agreement on Trade in Services (GATS) permits trade

[18] United Nations, 'The Right to Privacy in the Digital Age', Resolution adopted by the General Assembly on 18 December 2013, 68/167, available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.
[19] United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age (an Overview)', available at: http:// www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.
[20] Joseph A. Cannataci, 'Report of the Special Rapporteur on the Right to Privacy', UN General Assembly Seventy-Fifth Session, A/75/147, 27 July 2020.

restrictions that are necessary for 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts', specifying that 'such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services'. As more business models and practices move onto the digital platform and data become increasingly shared and exchanged on an international scale, its relevance in international trade intensifies. Since data are gathered, digitized, stored, and moved on a truly global scale by a multitude of parties, restrictions and regulations concerning data directly affects global trade. Data protection is directly related to trade in goods and services in the digital economy – as too little protection can create negative market effects through affecting consumer confidence; and too much can overly restrict business activities and trade.

65. The cross-border supply of digital services inevitably includes cross-border flow of data required for the service, such as consumer data or business data. Consequently, data localization measures which restrict or *de facto* prohibit cross-border trade in services can be assessed under the General Agreement on Trade in Services (GATS) framework, and may raise questions as to whether data localization measures violate the core principles of GATS. Provisions prohibiting data localization have become increasingly common in recent FTAs. More and more countries are willing to accept such provisions in their regional and bilateral trade agreements. Thus, so far only FTAs have binding obligations prohibiting data localization measures, with data localization measures not being explicitly deemed trade restrictive under GATS.

3) Regulating Online Harmful Content

66. Like any other communication technologies, the Internet carries an amount of potentially harmful or illegal contents that can be misused as a vehicle for criminal activities.

67. Although many different forms of content can fall under the umbrella term 'unlawful or harmful content', the very different nature of the content means that a single response is unlikely to be effective. For example, a number of different forms of content may be prohibited under international human rights law (which we term 'unlawful content') or which may be legitimately prohibited under the limited exceptions to the right to freedom of expression (which we term 'harmful content'), including terrorism-related and extremist content, hate speech, online gender-based violence, 'fake news', disinformation and propaganda. There are many others: child sexual abuse, certain forms of pornography, incitement to violence or hatred, copyrighted material. The harms that result from these forms of content vary greatly, and while some of these forms of content can be relatively clearly identified (such as child sexual abuse), others - such as extremist content or hate speech - are less easy to define.

68. These differences mean that different responses may be required from both States and platforms. Different stakeholders may need to be engaged and different approaches in terms of attaching liability may need to be considered. In short, the degree to which algorithms or automation may be of use in regulating content may vary. Just as there are different responses

to, for example, copyrighted material and hate speech, when it appears offline, so different responses are required when they appear online. These responses may need to go beyond simply restricting or removing the content, and address the causes of the particular problem, including through offline interventions such as appropriate education, improved digital literacy, funding for programmes tackling harmful behaviour.

69. In terms of illegal and harmful content, it is also crucial to differentiate between content which is illegal and other harmful content. For example, it would be dangerous to amalgamate separate issues such as children accessing pornographic content for adults, and adults accessing pornography about children. Priorities should clearly be set and resources mobilised to tackle the most important issues, which is the fight against criminal content - such as clamping down on child pornography, or use of the Internet as a new technology for criminals.

70. Therefore, it is clearly evident that online content regulation, including the regulation of illegal and harmful content can be quite tricky, as part of such content may be more manifest or easily identifiable like propaganda that incites racism, conspiracy theories, violence and radicalization; however, a lot of this content may be much subtler. As governments worldwide increasingly localize data and resort to monitoring or even removing user-generated content, discussions on the global platform, especially the UN[21] has largely focused on State regulation of online content where dissenting views are no longer heard; with the conclusion that over time this can undermine the basis for shared values and tolerance in a society, tearing at the fabric of democracy itself.

71. The World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) has called attention to the role of Artificial Intelligence (AI) in the selection of information and news that people read, the music they listen to and the decisions they make, as well as their political interaction and engagement. Underlying this point is a concern that the AI systems used by technology companies are "black boxes" that open an information chasm between the technology companies and everybody else, including policymakers and regulators.[22]For example, as a result of the increasing reliance on AI-generated trending topics, the World Health Organization had to battle an "infodemic" alongside COVID-19 because many people at risk of contracting the virus were unaware of how much information about the pandemic was incorrect, deliberately misleading or malicious.

72. In another example, the United States Federal Bureau of Investigation reported a four-fold increase in the volume of cyber fraud; scammers took advantage of the crisis and offered fake advice on COVID-19 to induce recipients to click on their links, which allowed them to download malware and capture personal and financial information. Other increasingly pressing concerns include the concentration of the ownership of platforms, the millions of people left behind who are unconnected or lack the digital skills to be competitive, and the

[21] See *The Age of Digital Interdependence, Report of the United Nations Secretary-General's High-level Panel on Digital Cooperation* (New York, 2019), p.17. Available at https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf; E. C. Rattray, 'Media and Information Literacy in an Age of Uncertainty', *UN Chronicle*, 3 Dec 2020, available at: https://www.un.org/en/un-chronicle/media-and-information-literacy-age-uncertainty; and 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', United Nations General Assembly, A/HRC/38/35, 6 April 2018.

[22]Urs Gasser and Virgilio A.F. Almeida, 'A layered model for AI governance', *IEEE Internet Computing*, vol. 21, No. 6 (November, December 2017), pp. 58–62, available at https://dash.harvard.edu/handle/1/34390353.

fact that most media regulatory frameworks now lag far behind in the new world of accelerating technological change. For example, most regulation still operates exclusively at the national level, even though local firms are now competing with vastly bigger and largely unregulated foreign providers. Regulators need to take on a new role in ensuring that citizens can acquire the knowledge and skills needed to fully utilize digital resources while guarding against malicious, harmful and inappropriate content.[23]

73. The 2018 Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression - calling for States and companies to apply international human rights law at all stages of online content regulation: from creating rules about what content should be taken down, to conducting due diligence about how changes to platforms affect human rights, to providing remedies for people harmed by moderation decisions - is the first UN report to examine the regulation of user-generated online content. This move comes in the face of a global increase in governmentally imposed obligations to monitor and remove user-generated content. The Special Rapporteur in his Report recommends that States must adopt smart online regulation measures, and not heavy-handed viewpoint-based regulation, focused on ensuring company transparency and remediation to enable the public to make choices about how and whether to engage in online forums, and that they should refrain from imposing disproportionate sanctions, whether heavy fines or imprisonment, on Internet intermediaries, given their significant chilling effect on freedom of expression.[24]

74. It is well-established and accepted that human rights apply online as well as offline. The UN General Assembly has said that "the same rights that people have offline must also be protected online" (UN Doc. A/RES/68/167, Para 3) and the Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression have regularly stated that the same international human rights standards that apply to offline forms of freedom of expression apply equally to new communication technologies such as the internet (see, for example, UN Doc. A/HRC/17/27, Para 21). But these general statements only take us so far when it comes to the question of the scope of the right to freedom of expression online, particularly when it comes to social platforms. These platforms enable a wide range of forms of online expression ranging from globally accessible content (such as tweets on Twitter) to content accessible only to certain permitted individuals (such as posts on Facebook accessible only to 'friends'). While the content posted via these examples are regulated by the company's Terms of Service (or Community Standards or however otherwise termed), there are also opportunities for individual users themselves to regulate content. For example, Facebook enables individuals to establish both open and closed groups and to moderate posts that members make within these groups, either by requiring approval from an administrator before a post is published, or by being able to delete posts which have already been published.

75. If all of these forms of online expression are protected under the right to freedom of expression, this raises difficult questions about the responsibility for ensuring that the right is not restricted in a way which is incompatible with international human rights law. For

[23] E. C. Rattray, 'Media and Information Literacy in an Age of Uncertainty', *UN Chronicle*, 3 Dec 2020, available at: https://www.un.org/en/un-chronicle/media-and-information-literacy-age-uncertainty.
[24] 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', United Nations General Assembly, A/HRC/38/35, 6 April 2018.

example, as the ultimate obligation to ensure the protection of human rights falls upon the State, is it necessary for governments to legislate or otherwise involve themselves on questions of content regulation by private individuals who are administrators of private social media groups? It also raises another question about the responsibility of the individual who exercises freedom of expression online to respect the human rights of others and to abide by relevant laws and regulations. As regulators of online activities, governments should ensure a balance between freedom of expression online and corresponding responsibilities of the individuals exercising freedom of expression online.

76. As presently there is no international convention that regulates online harmful content, it is broadly dealt with under national legislations. Jurisdiction is another big challenge in regulating online harmful content because cyber criminals are generating content on servers in jurisdictions where such content is out of the purview of regulation, as States remain divided on the approach of regulating online harmful content. There is an urgent need for international regulations to curb and contain online harmful content, as with the advent of new technologies that govern our daily lives, like AI and Blockchain, the threat of online harmful content poses a threat to the entire international community more than ever before. In the meanwhile, it is also imperative that States refrain from curbing online freedom of opinion and expression, while regulating online harmful content.[25]

4) Peaceful Use of Cyberspace

77. The international community ought to observe the purposes and principles enshrined in the UN Charter in real earnest, particularly prohibition on the threat or use of force and peaceful settlement of disputes, in order to ensure peace and security in cyberspace.

78. The legality of any resort to force by States, whether through cyber or kinetic means, is governed first by the law on the use of force (or *jus ad bellum*) as reflected in the UN Charter. It requires States to refrain from the threat or use of force while preserving the right of individual or collective self-defense in response to an armed attack. It also permits the UN Security Council to sanction the use of force to maintain international peace and security. The aim of IHL or *jus in bello*, that applies during an armed conflict, on the other hand, is to mitigate suffering, by protecting those who are not, or are no longer, participating in

[25] To address the dilemmas of regulation and moderation of online content, UN Human Rights Office of the High Commissioner (OHCHR) has proposed five actions for States and companies to consider:
First, UN OHCHR urges that the focus of regulation should be on improving content moderation processes, rather than adding content-specific restrictions.
For example, when faced with complex issues, people should be making the decisions, not algorithms.
Second, restrictions imposed by States should be based on laws, they should be clear, and they should be necessary, proportionate and non-discriminatory.
Third, companies need to be transparent about how they create and moderate content and how they share information, and States need to be transparent about their requests to restrict content or access users' data.
Fourth, users should have effective opportunities to appeal against decisions they consider to be unfair, and independent courts should have the final say over lawfulness of content.
Finally, civil society and experts should be involved in the design and evaluation of regulations.
See 'Moderating Online Content: Fighting Harm or Silencing Dissent', UN OHCHR, 23 July 2021.

hostilities, and by restricting the means and methods of warfare that parties to armed conflicts may employ.

79. The International Court of Justice has opined that Articles 2(4) and 51 of the UN Charter regarding the prohibition on use of force and self-defence, respectively, apply to 'any use of force, regardless of the weapons employed'.[26] Nevertheless, there are a number of legal issues associated with the application of international law on the use of force, to cyber-attacks.

80. Article 8 of the Articles on the Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission in 2001 provides that 'the conduct of a person or a group of persons shall be considered as an act of State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct'. A less stringent threshold – 'overall control' was laid down by the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the *Tadić*case, wherein it stated that for attribution, it is sufficient that the State has a 'role to play in organizing, coordinating or planning the actions of the military group, in addition to financing, training and equipping or providing operational support to that group… regardless of any specific instructions by the controlling State concerning the commission of each of those acts'.[27]Few commentators have advocated for the adoption of the *Tadić Test* in cases of cyber-attack, given its inherently clandestine nature and the technical difficulty in identifying the authors of the attack.[28] Rule 6 of the Tallinn Manual 1.0 states that 'a State bears international legal responsibility for a cyber-operation attributable to it and which constitutes a breach of an international obligation'.[29]

81. Another issue relates to the precise modalities governing the use of force in cases of self-defence. In this context, it will have to be examined that under what circumstances cyber operations can amount to: a) an internationally wrongful act of threat or use of force; and b) an 'armed attack' justifying the resort to necessary and proportionate force in 'self-defence'. Rule 11 of the Tallinn Manual 1.0 suggests in this regard that 'A cyber-operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of use of force'. It is, therefore, clear that the application of international law on use of force to cyberspace is by no means a straightforward task, and requires more deliberations among States for any consensus to be reached.

82. ICRC concerns itself with any new weapon, and on the humanitarian consequences of its use and its compatibility with IHL. While the military potential of cyberspace is not yet fully understood, cyber-attacks against electoral systems, transportation systems, electricity networks, dams, and chemical or nuclear plants have had been technically possible. Such attacks have had wide-reaching humanitarian consequences. It is therefore, urgent to take practical steps with a view to clarifying the limits that IHL already imposes on the resort to cyber operations as a means or method of warfare, and also to consider humanitarian contingency plans in the event of such attacks occurring. The ICRC defines cyber-warfare as

[26]*Nuclear Weapons Advisory Opinion*, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (July 8), para. 39.
[27]*Prosecutor* v. *Tadić*, ICTY, Case no. IT-94-1-A, Appeals Chamber Judgment, 15 July 1999, para. 117.
[28] S.J. Shackelford, 'From Nuclear War to Net War: Analogizing Cyber-Attacks in International Law', *Berkeley Journal of International Law*, 27(2009), p. 192.
[29] Tallinn Manual 1.0, (CUP, 2013), pp. 37-38.

operations against a computer or computer system through a data stream or computer code, when used as a means or method of warfare in an armed conflict.

83. While IHL treaties do not expressly prohibit or regulate cyber warfare, there are limitations under IHL when parties to a conflict resort to cyber operations. This is made clear in the obligation to undertake a legal review of new weapons, to determine if their use is prohibited by international law as stipulated under Art. 36 of the First 1977 Additional Protocol to the Geneva Conventions. Such reviews are indeed essential to ensure that new weapons comply with existing law including IHL norms and this is precisely because such norms apply to new weapons. All States have an interest in assessing the legality of new weapons regardless of whether they are party to Additional Protocol I.

84. There is an increasing concern in many countries about safeguarding essential civilian infrastructure against cyber-attacks. Facilities providing potable water and electricity networks that serve civilian populations, public health infrastructure, dams, and nuclear plants are civilian objects and enjoy special protection under IHL. The application of IHL to cyber warfare means that attacks against such objects are prohibited.

85. However, the application of IHL to cyber-warfare is not without its challenges. The first challenge concerns the interconnection of cyberspace with the principles of distinction and proportionality related to the conduct of hostilities. And yet it must be assessed to meet the prohibition of indiscriminate and disproportionate attacks which is an obligation under IHL. Secondly, the notion of "attack", which is fundamental to the application of the rules on the conduct of hostilities poses a significant challenge. Indeed, most of the rules mentioned earlier apply to "attacks", which are defined by the First 1977 Additional Protocol as "acts of violence against the adversary, whether in offence or in defense." At the heart of this issue is the question - what amounts to an "act of violence" in cyber space? The final challenge is the anonymity in cyberspace, which complicates the ability to attribute aggressive activities to perpetrators. If the perpetrator of a cyber-attack cannot be identified it may be difficult to determine if IHL is even applicable to the operation. More and more concerted efforts by States would be required to ascertain and determine the applicability of IHL to cyberspace.

86. Many States today are of the opinion that the purpose of studying cyberwarfare would be to try and stop it, including the ways and means of raising of awareness, and capacity-building within States, especially in the matter of determining cyber-threats in advance; and not to encourage arms-race. Nevertheless, what is also a fact of the matter is that cyber-operations cannot and ought not to be allowed to be carried out in a legal vacuum. Only through collective efforts can we ensure that the obligation to respect IHL remains aligned with developments in the technology of warfare.

IV. Observations and Comments of the AALCO Secretariat

87. Digital technologies are rapidly transforming societies and economies, simultaneously advancing the human condition and creating profound and unprecedented challenges. In this scenario, the ultimate objective of the application of international law to regulate cyberspace is undoubtedly to steer the usage of digital technologies in a way that can contribute to the

achievement of the Sustainable Development Goals within States[30], in order to maximise benefits to society and minimise harms.

88. The challenges that the current 'Digital Age' gives rise to are multi-faceted and rapidly evolving. Negative trends in the digital domain could undermine international security and stability, place strains on economic growth and sustainable development, and hinder the full enjoyment of human rights and fundamental freedoms. These trends include the growing exploitation of ICTs for malicious purposes. The current global health crisis has underscored the fundamental benefits of ICTs and our reliance upon them, including for provision of vital government services, communicating essential public safety messages, developing innovative solutions to ensure business continuity, accelerating research, and helping to maintain social cohesion through virtual means. At the same time, the COVID-19 pandemic has demonstrated the risks and consequences of malicious activities that seek to exploit vulnerabilities in times when societies are under enormous strain. It has also highlighted the necessity of bridging digital divides, building resilience in every society and sector, and maintaining a human-centric approach.

89. In order to meet these challenges, there is an urgent requirement that citizens, civil society, governments, academia and the private sector work together in more effective and inclusive ways. We urgently need new forms of digital cooperation to ensure that digital technologies are built on a foundation of respect for human rights and provide meaningful opportunity for all people and nations.

90. Most current mechanisms of digital cooperation are primarily local, national or regional. However, digital interdependence also necessitates that we strengthen global digital cooperation mechanisms to address challenges and provide opportunities for all. The Internet Governance Forum or IGF is currently the main global space convened by the UN for addressing internet governance and digital policy issues. The Fifteenth Annual Meeting of the IGF in 2020 was hosted online by the United Nations under the overarching theme *Internet for human resilience and solidarity*. The programme was built around four main thematic tracks: (1) Data; (2) Environment; (3) Inclusion; and (4) Trust. One of the main outcomes of the meeting was that the COVID-19 pandemic revealed that even though many governments and private sector entities had data frameworks and policies, they were not adequate during a crisis, when data needed to be shared in real-time and needed a high degree of accuracy. It was also stated that accuracy in data collection, particularly in times of crisis, does not have to compromise privacy, whether it be personal privacy or the collective privacy of society. Establishing legal and ethical frameworks for information processing are vital for establishing transparency and accountability and for preventing data-driven technologies from deepening existing inequalities. These frameworks underpin the notion of informed consent – individuals can make meaningful decisions about data sharing knowing that their data will not be used for purposes other than stated purposes. Further, the benefits of data-driven technologies should be accessible to all, not just governments and the private sector, but also to communities and individuals. To enable this, people need access to digital devices

[30] For a more detailed account of the inter-relation between Digital Cooperation and the achievement of Sustainable Development Goals, see 'Fostering Digital Transformation and Global Partnerships: WSIS Action Lines for Achieving SDGs', WSIS Forum 2020 Outcome Document, 29 October 2020, available at: https://www.itu.int/net4/wsis/forum/2020/Files/outcomes/draft/WSISForum2020_OutcomeDocument_DRAFT-20201204.pdf.

and connectivity, as well as the digital literacy skills to make full use of data-driven technologies.[31]The Sixteenth Annual IGF meeting will be hosted by the Government of Poland in Katowice from 6-10 December2021, under the overarching theme: Internet United.

91. Recognizing the transnational nature of Cyberspace and the importance of establishing a framework of cyber governance consistent with the principles of international law, AALCO and its Member States have taken this topic with utmost seriousness. AALCO's approach on the topic has focused on the need to clarify international law norms on the topic while exploring the possibility of further expanding these norms in light of new technological developments while strongly encouraging responsible State behaviour in cyberspace.

92. In this regard, the AALCO Secretariat urges the Member States to submit their responses to the Rapporteur's questionnaire in preparation of the Rapporteur's Report on 'Special Need of the Member States for International Cooperation against Cybercrimes', as well as to the Secretary-General's 'Proposal of the Consensual Basic Principles of International Law Applicable in Cyberspace', so that a tangible outcome of the AALCO deliberations on the topic may emerge.

[31] 'Draft IGF 2020 Summary', Internet Governance Forum – Fifteenth Meeting, 17 November 2020, available at: https://www.intgovforum.org/multilingual/filedepot_download/10794/2357.