AALCO/54/BEIJING/2015/SD/S17

For official use only

ASIAN-AFRICAN LEGAL CONSULTATIVE ORGANIZATION

INTERNTIONAL LAW IN CYBERSPACE

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

INTERNATIONAL LAW IN CYBERSPACE

(Deliberated)

CONTENTS

INTERNATIONAL LAW IN CYBERSPACE

I. Introduction

A. Background

1. With the advent of information age, cyberspace has become a new domain for human interaction and an integral part of the analysis of the contemporary international relations. The technology's hybrid character consists of a transnational virtual structure, with information travelling through undersea cables and between physical devices located within and beyond the territories of nation-states. Today a third of the world's population has access to the Internet. The ubiquity of Internet transformed the way we communicate and search information and irreversibly altered the way we conduct our daily businesses. It has brought unprecedented opportunities to the advancement of humanity. It is estimated that the internet accounted for more than 20 percent of GDP growth of world's major economies over 2008-12 period. The benefits, needless to elaborate, goes far beyond economic growth—improved access to education, reduction of poverty, greater access to information and so on.

2. Unlike other strategic domains—land, sea, air and space—cyberspace is virtual and its very structure can therefore be changed. This unique feature of cyberspace poses considerable challenges to any attempts to regulate them within the territorial boundaries of nation-states. In fact, there is considerable disagreement on whether and to what degree cyberspace can be controlled generally and on whether leadership is possible, not only by states but by any hierarchically organised actor. Several argue that the open, minimalist and decentralised design of cyberspace, governed by a network of actors including private companies and non-governmental entities fundamentally undermines leadership by states and limits the points of control. Others argue that state leadership is possible and that cyberspace is increasingly being regulated through state authority as many examples demonstrate. The existing Internet governance regime has often been framed as a 'multi-stakeholder-model', which consists of governments, private companies and non-governmental organisations without an inherent hierarchy among the three.[1] A multi-stakeholder model is further understood as 'the opening of state-based international organizations to participation by "stakeholders" besides governments'.

3. However, in practice this ideal-typical multi-stakeholder model features the anomaly of the historical US government's leadership and the continuing contractual relationship between its Department of Commerce and Internet Corporation for Assigned Names and Numbers (ICANN). Some of the Member States of AALCO have been cognizant of this reality and have been arguing for the establishment of a UN centric model of internet governance with International Telecommunication Union (ITU) at its centre. This appears to be a distant possibility, as is evident from the result of recently concluded

[1] MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 7 (2010).

ITU's Plenipotentiary Conference 2014 wherein the position of the developed nations prevailed.[2]

4. Nonetheless, from the standpoint of international rule of law, the novelty of the so-called "fifth domain" does not preclude it from traditional rules and principles of international law. The fundamental tenet of in international law, i.e., state sovereignty is no exception and is intrinsically linked with internet governance. Despite cyberspace possessing many characteristics of "global commons", the state practice gives ample evidence of nations exercising their jurisdiction in regulating the conduct of its citizens in cyberspace. Lately, the exercise of sovereignty has been validated in many international forums as well. However, this entails corresponding obligations to respect and uphold fundamental freedoms of its citizens in cyberspace.

5. Cyber security is another area which is well discussed in international legal discourse.[3] Cyber security broadly refers to a state's ability to protect itself and its institutions against cyber threats. The major challenge to governments is to ensure that its institutions and people are primarily protected from cyber attacks and espionage on the Internet. Governments are investing significant resources to improve their cyber capabilities and reinforcing their defenses against impending cyber attacks on critical assets.[4] The recent revelations made by Edward Snowden, a computer analyst turned whistleblower, exposed the extent of cyber espionage targeting sovereign functions of many States. Further, burgeoning cyber crimes perpetrated by non-state actors including financial theft and other cross border crimes are threatening national security and financial health. A report estimates the annual damage to the global economy to be at $ 445 billion.[5]

B. Deliberations at the Fifty-Third Annual Session

6. It is roughly against this broad background that People's Republic of China proposed "International Law in Cyberspace" as an agenda item to be deliberated at the Fifty-Third Annual Session of AALCO held in Tehran in 2014 and it was accepted by consensus. Statements were made by the following Member States— People's Republic of China, Japan, Islamic Republic of Iran and Nigeria. The delegation of People's Republic of China, in its statement, highlighted the following issues concerning international law in cyberspace: (1) significance of principles of sovereignty and non-interference in cyberspace and the need to balance right to speech and expression and cyber security; (2) Peaceful use of cyberspace and prevention of cyber militarization; (3) international rules for combating cyber crime and (4) development and application of international rules for

---

[2] *See* Monika Ermert, *ITU Plenipotentiary Conference: Internet Governance Diplomacy on Display*, available at http://www.ip-watch.org/2014/11/05/itu-plenipotentiary-conference-internet-governance-diplomacy-on-display/

[3] *See generally* Mary Ellen O'Connell, Cyber Security and International Law, CHATHAM HOUSE (2012), available at:
<http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf>

[4] *See generally* Pierluigi Paganini, *Beware the Militarization of Cyberspace*, http://www.foxnews.com/tech/2014/12/18/beware-militarization-cyberspace/

[5] http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

cyberspace and the significance of the UN as the best forum for discussing and settling those norms and rules. The delegate of Japan while welcoming the proposal to develop a cybercrime convention at the UN, cautioned against duplication of efforts which may result in creating rules very similar to Budapest Convention. The delegate of Islamic Republic of Iran pointed out the permeating nature of cyber attacks vitiating some of the well-established principles of international law including inviolability of sovereignty and territorial integrity in the real world. The delegate of Nigeria expressed his State's concerns with respect to privacy and use of internet to promote terrorism.

7. The Resolution (AALCO/RES/53/S17) adopted pursuant to the deliberations recognized the need for developing and applying consistent international rules for cyberspace and called upon Member States for their communication and cooperation on this subject.

C. Issues for focused deliberation at the Fifty-Four Annual Session of AALCO

I. The necessity and suitability of a UN Centric Governance model for cyberspace.

II. Importance of balancing sovereign rights of the States and fundamental freedoms of speech and expression of its citizens in cyberspace.

III. Significance of the existing rules of war (jus ad bellum and jus in bello) in regulating state conduct in cyber warfare.

IV. Burgeoning transnational cyber crimes and the need for a multilateral treaty to effectively prevent its escalation.

II. Internet Governance, Sovereign Rights and Duties

8. Internet governance, in general terms, is the development and application of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. DeNardis states that "Internet Governance generally refers to policy and technical coordination issues related to the exchange of information over the Internet"[6] The Internet, in its early stages, developed and spread without direction from intergovernmental processes, such as the ITU, and without generating rules of international law. Eventually, as mentioned earlier, Internet governance evolved through multi-stakeholder processes in which state and non-state actors collaborated on managing technical and operational tasks, such as standardizing communication protocols and managing names and numerical addresses on the Internet.

9. When ITU members adopted the International Telecommunications Regulations (ITRs) in 1988, the Internet had not yet become a global communications, social, economic, and political phenomenon. The ITRs focused on the interconnection and interoperability of existing communication services and replaced the Telegraph Regulations and Telephone Regulations the ITU adopted in 1973. The ITRs contained general principles rather than detailed rules that formed a pragmatic, flexible framework for international cooperation. As the Internet expanded, many countries expressed

[6] Laura DeNardis, *The Emerging Field of Internet Governance*, YALE INFORMATION SOCIETY PROJECT WORKING PAPER SERIES (September 17, 2010).

concerns about multi-stakeholder governance, including that it gave the United States dominance over the Internet and its development. These countries sought to bring Internet governance within intergovernmental processes and international law.[7] In the lead-up to the first phase of World Summit on the Information Society (WSIS) in December 2003, China, with support from developing countries, proposed creating an international Internet organization and adopting an Internet treaty.

10. Disagreements at the WSIS in 2003 between proponents of the multi-stakeholder approach and advocates of more governmental and intergovernmental control led the WSIS to ask the UN Secretary-General to establish a Working Group on Internet Governance (WGIG) in 2004. When confronted by the same disagreements, the WGIG recommended creation of an Internet Governance Forum (IGF). The second phase of the WSIS in 2005 established the IGF as a multi-stakeholder discussion forum with no decision making authority. The ITU decided in 2006 to review the ITRs in light of the changed international telecommunications environment and to hold a World Conference on International Telecommunications in 2012 to amend the ITRs.[8]

A. The World Conference on International Telecommunications (WCIT 2012)

11. In the lead-up to the WCIT-12, proponents of the multi-stakeholder model argued that the ITU and certain ITU members were using the WCIT-12 to bring Internet governance under governmental and intergovernmental control, with dire consequences for innovation, commerce, development, democracy, and human rights. Although ITU Secretary-General Hamadoun Toura stated the WCIT-12 would not address Internet governance, proposals by ITU members included changes focused on the Internet and how it is governed. For example, Russia proposed a new article on the Internet, which included a provision aimed at the multi-stakeholder model: Member States shall have equal rights to manage the Internet, including in regard to the allotment, assignment and reclamation of Internet numbering, naming, addressing and identification resources and to support for the operation and development of the basic Internet infrastructure. Other proposed revisions included financing Internet communications, dealing with spam, and addressing computer and network security.

12. The WCIT-12 ended without consensus. Of the 144 delegations with voting rights at the WCIT-12, eighty nine signed the revised ITRs, including many African countries, Brazil, China, Indonesia, Iran, and Russia, while fifty-five did not, including Australia, members of the European Union (EU), Canada, Japan, and the United States. Before negotiations ended, the United States announced its opposition, based on what the revised ITRs contained concerning the Internet. Although the ITU Secretary-General indicated that the WCIT-12 would make decisions by consensus, active opposition by prominent countries demonstrated a lack of consensus leaving the ITU with an amended treaty both

[7] D.P. Fidler, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, ASIL INSIGHTS, Vol.17, Issue.6 (2013).
[8] *Id.*

supported and opposed by powerful countries and a significant proportion of its membership.[9]

B. Later Developments

13. On 7 October 2013, the Montevideo Statement on the Future of Internet Cooperation was released by the leaders of a number of organizations involved in coordinating the Internet's global technical infrastructure, loosely known as the "I*" (or "I-star") group. Among other things, the statement "expressed strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance" and "called for accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing". This enhanced desire to move away from a United States centric approach is seen as a reaction to the ongoing NSA surveillance scandal. The statement was signed by the heads of the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force, the Internet Architecture Board, the World Wide Web Consortium, the Internet Society, and the five regional Internet address registries (African Network Information Center, American Registry for Internet Numbers, Asia-Pacific Network Information Centre, Latin America and Caribbean Internet Addresses Registry, and Réseaux IP Européens Network Coordination Centre).

14. In April 2014, the Global Multi-stakeholder Meeting on the Future of Internet Governance (GMMFIG) Conference was hosted by a High-Level Multi-stakeholder Committee, composed of ministerial representatives of twelve countries (Argentina, Brazil, France, Ghana, Germany, India, Indonesia, South Africa, Republic of Korea, Tunisia, Turkey, and the United States of America) and 12 members of the multi-stakeholder international community. The meeting produced a non-binding statement in favor of consensus-based decision-making. It reflected a compromise and did not harshly condemn mass surveillance or include the words “net neutrality”, despite initial support for that from Brazil. The final resolution says ICANN should be under international control by September 2015.[10]

15. A minority of governments, including Russia, China, Iran and India, were unhappy with the final resolution and wanted multilateral management for the Internet, rather than broader multi-stakeholder management. That would give mainly governments decision-making power, for example via the United Nations, and be more likely to encourage individual nations to control their national domains inside walled gardens which could be more easily monitored and filtered, as with telephone systems influenced by the International Telecommunication Union.

[9] For a detailed discussion, *see* http://www.itu.int/en/wcit-12/Pages/default.aspx

[10] *See* Philip Corwin, *NETmundial Multi-stakeholder Statement Concludes Act One of 2014 Internet Governance Trifecta*, available at <http://www.circleid.com/posts/20140504_netmundial_multistakeholder_statement_concludes_act_one_of_2014/>

C. ITU Plenipotentiary Conference 2014

16. In the ITU Plenipotentiary Conference 2014, held in Busan, Republic of Korea, it was expected that ITU would be mandated with a greater role in internet governance. However, this did not materialize. The Conference passed a set of internet-related resolutions that preserves the limited status quo of involvement of the ITU.[11] In the lengthy and intense discussions the Working Group of the Plenary found compromises for what had looked like rather extreme proposals from different ends. For instance, Russia proposed that ITU begin allocating internet protocol (IP) addresses, which is a function already performed by other non-intergovernmental organisations. The Arab states had submitted proposals that would have strengthened the role of governments in making decisions about the internet and would have given the ITU a role in developing legal and policy frameworks to combat illegal international online surveillance. Brazil made proposals for ITU to work on online privacy issues.[12]

17. According to the reports, the biggest discussion erupted over a proposal from India that favoured undertaking a series of studies that in effect pushed for a localisation of networking.[13] One study would "explore the development of naming and numbering system from which the naming and numbering of different countries are easily discernible," another one "recommend a system that ensures effectively that traffic originating and intended to be terminating in the same country remains within the country." These ideas were tantamount to redesign of existing telecommunications networks or protocols" and an expansion of the "ITU mandate," which was widely opposed by developed nations. The Indian proposals as well as a proposal from the Arab group, which demanded the ITU to start discussing a legal instrument to protect internet users against mass surveillance by intelligence agencies, can perhaps both be seen as fallout from the revelations of Edward Snowden.

18. All the extreme positions were erased in the negotiations. A bigger mandate for the government-led ITU in internet governance was widely opposed by the Global North reiterating their persistent objection to making any substantial rearrangement of the existing framework. But green light was given "to continue to undertake activities on international Internet related public policy issues within ITU mandate in collaboration and cooperation with relevant organizations and stakeholders, as appropriate, with special attention to the needs of developing countries" as it is introduced in the updated resolution 102. Also the two big regional blocs – industrialised and developing countries – agreed on an acknowledgement that governments, too, are "stakeholders" and "continue to play a very important role in the expansion and development of the internet, for example through investments in infrastructures and services."

---

[11] Monika Ermert, *ITU Plenipotentiary Conference: Internet Governance Diplomacy on Display*, available at http://www.ip-watch.org/2014/11/05/itu-plenipotentiary-conference-internet-governance-diplomacy-on-display/

[12] For details, *see* http://www.itu.int/en/plenipotentiary/2014/Pages/default.aspx

[13] *Supra* note 10.

19. A new dedicated resolution on promoting internet exchanges and guiding principles for them could be agreed upon and was withdrawn by Argentina and other Latin American proponents in exchange for including strong references on ITU work on internet exchanges in the updated internet resolutions 101 and 102. Sovereignty over country-code top-level domains (ccTLDs) explicitly was introduced based on the text of the Tunis Agenda of the 2003-2005 World Summit on the Information Society (WSIS). This was a fix requested by those not completely at ease with the US-based Internet Corporation for Assigned Names and Numbers (ICANN), which has technical oversight of the domain name system.

20. The next substantive meeting to discuss technology and internet issues in the UN is the General Assembly's special high-level meeting in December 2015. This meeting will review a decade of activities since the World Summit on the Information Society was held in Tunis in 2005.

D. Cyber Sovereignty and State Responsibility

21. The arguments favouring greater state control over internet governance primarily hinges on the extension of state sovereignty to cyberspace. Irrespective of the various theories on the legal function of territory there is widespread agreement that according to the principle of territorial sovereignty a State exercises full and exclusive authority over its territory. Max Huber, in the Palmas Island Arbitration award, has affirmed this general principle as follows: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusivity of any other States, the functions of a State".[14]

22. According to the International Court of Justice, "between independent States, respect for territorial sovereignty is an essential foundation of international relations."[15] Territorial sovereignty therefore implies that, subject to applicable customary or treaty rules of international law, the respective State alone is entitled to exercise jurisdiction, especially by subjecting objects and persons within its territory to domestic legislation and to enforce these rules. Moreover, the State is entitled to control access to and egress from its territory. The latter right seems to also apply to all forms of communication. Territorial sovereignty protects a State against any form of interference by other States. the rights of other States, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory.

23. Despite of the correct classification of 'cyberspace as such' as a *res communis omnium* State practice gives sufficient evidence that cyberspace, or rather: components thereof, is not immune from sovereignty and from the exercise of jurisdiction.[16] On the one hand, States have exercised, and will continue to exercise, their criminal jurisdiction

[14] Wolff Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, available at <https://ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf>

[15] ICJ, The Corfu Channel Case (Merits), ICJ Rep., 1, at p. 35 (1949).

[16] *Supra* note 13.

vis-à-vis cyber crimes and they continue to regulate activities in cyberspace. On the other hand, it is important to bear in mind that "cyberspace requires a physical architecture to exist". The respective equipment is usually located within the territory of a State. It is owned by the government or by corporations. States have continuously emphasized their right to exercise control over the cyber infrastructure located in their respective territory, to exercise their jurisdiction over cyber activities on their territory, and to protect their cyber infrastructure against any trans-border interference by other States or by individuals.

24. The UN Group of Governmental Experts on Information Security 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." (para.20) However, as embodied in Article 19 of the Universal Declaration of Human Rights, freedom of expression and information must be promoted without exception. The exercise of sovereignty by any State must be subjected to this right. A corresponding recognition of freedom of expression has been expressed by the WSIS in the Declaration of Principles, paragraphs 4, 55 and 56-59 and Action Plan, paragraph 24 adopted during the Summit of the first phase of the WSIS in Geneva, December 2003.[17]

25. Nevertheless, with respect global management of the Internet, "multi-stakeholder" seems to be the dominant model. This view is reiterated in Declaration of Principles adopted at the World Summit on the information Society held in December 2013. While recognizing the sovereign rights of States on Internet-related public policy issues, it emphasized the importance of private sector and intergovernmental organizations in the development and coordination of internet and related public policy issues.[18]

III. Cyber Security— Militarization of Cyberspace and Cybercrimes

26. Cyber security has emerged as another central focus of contestation. We understand cyber security here as a state's ability to protect itself and its institutions against cyber threats. Militaries around the world have become more and more interested in the Internet since it expanded and vulnerabilities increased. Critical national infrastructures that depend upon computer networks have become increasingly vulnerable to cyber-attacks. Moreover, the cyberspace is becoming ever more susceptible to cyber crimes and espionage. Given the magnitude of threats posed by state and non-state actors, this section briefly discusses the applicability of existing rules and principles of international law in addressing these concerns.

[17] Report on UNESCO Thematic Meeting for the Preparation of the Second Phase of the World Summit on the Information Society (WSIS 2005), available at <http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis_tunis_prep_cyberspace_report_en.pdf

[18] Document WSIS-03/GENEVA/DOC/4-E, 12 December 2013, Declaration of Principles, World Summit on the information Society. Paragraph 49.

A. Cyber Warfare and Espionage

27. The military reliance on computer systems and networks has increased exponentially, thus opening a "fifth" domain of war-fighting next to the traditionally recognized domains of land, sea, air and outer space. The term "cyber warfare", broadly speaking, refers to warfare conducted in cyberspace through cyber means and methods. For example, the infection of a belligerent adversary's computer network with a malicious virus would constitute an act of cyber warfare. There is only one cyber space, shared by military and civilian users, and everything is interconnected. According to the contemporary rules of International Humanitarian Law, the key challenges when resorting to cyber warfare are to ensure that attacks are directed against military objectives only and that constant care is taken to spare the civilian population and civilian infrastructure. Further, the expected incidental civilian losses and damage must not be excessive in relation to the concrete and direct military advantage anticipated by the cyber attack. If these conditions cannot be met, the attack must not be launched. These challenges underline the importance of States being extremely cautious when resorting to cyber attacks.

28. Without any doubt, existing international law governs state activities wherever they are carried out, including in cyberspace. However, applying pre-existing legal rules, concepts and terminology to a new technology entails their interpretation in view of the specific characteristics of the technology in question. Tallinn Manual on the International Law Applicable to Cyber Warfare serves as an important legal document in this regard.[19] It is an academic, non-binding study on how international law, in particular the jus ad bellum and international humanitarian law, apply to cyber conflicts and cyber warfare. The Tallinn Manual was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence by an international group of approximately twenty experts between 2009 and 2012.

29. The jus ad bellum is that body of law which governs the resort by states to force in their international relations. Today, the most important source of jus ad bellum is the UN Charter. The Charter is instrumental in determining in what circumstances, if any, cyber operations can amount to (1) an internationally wrongful threat or use of "force", (2) an "armed attack" justifying the resort to necessary and proportionate force in self-defence, or (3) a "threat to the peace", "breach of the peace" or "act of aggression" subject to UN Security Council intervention.[20] The Tallinn Manual presents some key conclusions on the "use of force" and state responsibility in cyberspace after careful examination of the Charter, customary international law and other relevant legal instruments:

- States may not knowingly allow cyber infrastructure located in their territory to be used for acts that adversely affect other States.

[19] The Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013.
[20] *See generally* Nils Melser, *Cyber Warfare and International Law*, UNIDIR Resources (2011).

- States may be responsible for cyber operations directed against other States, even though those operations were not conducted by the security agencies. In particular, the State itself will be responsible under international law for any actions of individuals or groups who act under its direction. For instance, a State that calls on hackers to conduct cyber operations against other States will be responsible for those actions as if it had conducted them itself.

- The prohibition on the use of force in international law applies fully to cyber operations. Though international law has no well-defined threshold for determining when a cyber operation is a use of force, the International Group of Experts agreed that, at a minimum, any cyber operation that caused harm to individuals or damage to objects qualified as a use of force.

- The International Group of Experts agreed that cyber operations that merely cause inconvenience or irritation do not qualify as uses of force.

30. Correspondingly, as mentioned above, International Humanitarian Law (IHL) or jus in bello, which imposes legal limits to wartime conduct, applies to cyber warfare. The use of cyber operations in armed conflict can potentially have devastating humanitarian consequences. When the computers or networks of a State are attacked, infiltrated or blocked, there may be a risk of civilians being deprived of basic essentials such as drinking water, medical care and electricity. If GPS systems are paralysed, there may be a risk of civilian casualties occurring – for example, through disruption to the flight operations of rescue helicopters that save lives. Dams, nuclear plants and aircraft control systems, because of their reliance on computers, are also vulnerable to cyber attack.[21] Networks are so interconnected that it may be difficult to limit the effects of an attack against one part of the system without damaging others or disrupting the whole system. All this calls for the application of IHL.

31. Chapters IV and V of the Tallinn Manual exclusively deal with the application of IHL to cyber warfare. The Manual upholds the classical dichotomy between international and non-international armed conflicts, and recognizes that cyber operations alone may constitute armed conflicts depending on the circumstances – notably on the destructive effects of such operations. In this regard, the manual defines a "cyber attack" under IHL as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."

32. Similarly, in the wake of reports on large-scale snooping on the foreign missions and other activities of many nations, cyber espionage factors in as a critical concern with respect to cyber security. While espionage has been the part and parcel of Cold War politics, thanks to technology, its sheer enormity and impunity today is unparalleled.

[21] Cyber attacks on the nuclear installations of Iran using “stuxnet” worm is a good example. *See generally* Michael
Kelly, *The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, <http://www.businessinsider.in/The-Stuxnet-Attack-On-Irans-Nuclear-Plant-Was-Far-More-Dangerous-Than-Previously-Thought/articleshow/26113763.cms>

Vienna Convention on Diplomatic Relations reaffirms the inviolability of diplomatic correspondence and casts a positive obligation on the host states to protect free communication on the part of the diplomatic mission for all official purposes (Article 27, VCDR). It even stipulates a third country's similar obligations when such communication is in transit (Article 40 (3), VCDR). The VCDR explicitly protects traditional diplomatic communications e.g. couriers, bags and wireless transmission.[22] It came into force when early forms of computers were still being developed and e-correspondence did not find a specific mention therein. However, Article 24 of VCDR states that the archives and documents of the mission "shall be inviolable at anytime and wherever they may be". Thus this provision amply covers email correspondence and data stored in hard disks and in the "cloud."

33. Further, Tallinn Manual clearly states that a state bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of international obligation (Rule 6). Cyber espionage of diplomatic correspondence thus involves specific violation of a treaty law (VCDR) and can be attributable to the state ordering it. The Manual says that any cyber activity undertaken by the intelligence, military, internal security, customs or other State agencies will engage state responsibility under international law if it violates an international legal obligation applicable to it.

B. Cyber Crimes and International Law

34. Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. Cyber crime can be broadly defined as crime committed against or targeting computers, or committed through use of computers or information communications technologies. So this could apply to a wide array of crimes throughout the world. During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed within a related workshop: Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[23]

35. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government

[22] *Vienna Convention on Diplomatic Relations Vienna*, 18 April 1961, 500 UNTS 95.

[23] *Crimes related to Computer Networks*, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners.

36. Given the less number of international legal instruments that can be used to deter the cyber crime, it becomes pertinent to question whether the antecedent customary law dealt with the issue of cyber crime. There is a body of customary international law reflecting the extensive and virtually uniform conduct of nation states during traditional warfare that is widely accepted and well understood the law of war. Unfortunately the application of the law of war to cyber crime is problematic because the actions and effects available to nations and non state actors in cyber space do not necessarily match up with the principles governing armed conflict and the anecdotal nature of the crime perpetration in cyber crimes problematizes the application of those basic principles on this grey area.

37. The proliferation of advanced technologies, the failure of international normative regime to device legal restraints on its usage and lack of effective monitoring mechanisms to regulate the cyber activities has contributed to the mounting problem of cyber crime. The potential threats of cyber crime have not only disrupted the normal individuals but also pose a great challenge to the policy makers, governments and media. Though the activities in cyberspace is *de jure* subject to the jurisdiction of an individual state, the technical intricacies involved in its communication pose a great challenge to international law. This problem is aggravated by failure of international law to bring the non state actors that have technological lead in cyber space under regulation by specific treaty based rules and has facilitated such non state actors to take advantage of the failed legal regime to continue their indulgence in perpetrating the crime. Even the developed countries, multinational companies and states have shown less interest in establishing an effective regulatory framework to thwart the criminal activities in cyber crime. For developing countries, finding response strategies and solutions to the threat of cybercrime is a major challenge. This necessitates one to ponder on to what extent the international legal regime is efficacious in regulating the cyber crime and how it is progressing towards addressing the security concerns of cyber space.

38. In this regard, the World Summit on the Information Society (WSIS) recognized the real and significant risks posed by inadequate cyber security and the proliferation of cybercrime.[24] The provisions of sections 108-110 of the WSIS Tunis Agenda for the Information Society, including the Annex, set out a plan for multi-stakeholder implementation at the international level of the WSIS Geneva Plan of Action, describing the multi-stakeholder implementation process according to eleven action lines and allocating responsibilities for facilitating implementation of the different action lines.[25] At WSIS, world leaders and governments designated ITU to facilitate the implementation of WSIS Action Line C5, dedicated to building confidence and security in the use of ICTs.

39. The Convention on Cyber Crime which is also called as Budapest Convention is the

[24] For more information on the World Summit on the Information Society (WSIS), *see* www.itu.int/wsis/

[25] The WSIS Tunis Agenda for the Information Society, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

only existing multilateral treaty that specifically addresses computer related crimes which came into force on July 1, 2004 and in addition, there exists an "Additional protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems". The Convention is designed to enhance the investigation and prosecution of cross-border computer related crimes by eliminating or reducing procedural and jurisdictional obstacles to international cooperation. But the inherited inadequacies and loopholes in the convention has rendered it weak in deterring the hackers. Cybercrime is an area of crime that is constantly changing.

40. In the 1990s, when the Convention on Cybercrime was developed, terrorist use of the Internet, botnet[26] attacks and phishing[27] either were not known or did not play as important a role as they do today, and could therefore not be addressed with specific solutions. The same is true with regard to procedural instruments. Interception of voice-over-IP (VoIP) communication, the admissibility of digital evidence and procedures to deal with the emerging use of encryption technology and means of anonymous communication are issues that are of great relevance to, but not addressed by, the Convention on Cybercrime. In its ten years of existence, the Convention has never been amended and, apart from the Additional Protocol on xenophobic material, no additional provisions or instruments have been added.[28]

IV. Comments and Observations of the AALCO Secretariat

41. The idiosyncratic nature of cyberspace demanded a *sui generis* model for its governance and the existing multi-stakeholder framework came into existence overtime in response. However, this framework, with predominant western control over it, is far from equitable. The developing States prefer a UN Centric model to balance this anomaly. At the recently concluded ITU plenipotentiary, discussions on internet governance were intense, but the outcomes were fairly insubstantial. It suggests that States are willing to concede only a little when it comes to protecting their interests in matters regarding governance of cyberspace. It seems States are ambiguous in stating their policy positions in proposals, but are more willing to let them go by the wayside as long as proposals by those with opposing views also are not incorporated. The legal, technical and institutional challenges posed by the issue of cyber security are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation. The Secretariat strongly believes that a multilateral and conciliatory approach, taking into account the demands of all stakeholders in internet governance while respecting sovereign rights of all States in regulating Internet in their jurisdictions, is the best way forward in future negotiations.

[26] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, *see* Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

[27] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from sea of Internet users.

[28] ITU, UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE 126 (2012).

42. In view of the novel character of cyberspace and in view of the vulnerability of cyber infrastructure and cyber components there is a noticeable uncertainty amongst governments and legal scholars as to whether the traditional rules and principles of customary international law are sufficiently apt to provide the desired answers to some worrying questions. It is, therefore, of utmost importance that States not only agree on the principal application of customary international law to cyberspace but also on a common interpretation that takes into due consideration the unique attributes of cyberspace. Hence it is necessary that governments continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace.

43. Further, the recent escalation in the militarization of cyberspace is alarming. Rise in cyber attacks on critical infrastructure of many States and cyber espionage on the activities of many States calls for a detailed deliberation on the legal rules applicable in such conduct. Tallinn Manual, which provides partial answers to these concerns, is a non-binding instrument. AALCO Member States, mindful of the vulnerabilities of their cyber infrastructure and susceptibility to cyber incursions by both State and non-State actors, should declare their commitment towards adherence to and enforcement of the UN Charter, international human rights instruments and International Humanitarian Law in their conduct in cyberspace.

44. Furthermore, in view of the singular characteristics of cyberspace, the fight against cybercrime necessitates a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law-enforcement agencies at the national level are allowed to investigate and prosecute cybercrime effectively. Capacity building is also critical for developing nations to effectively thwart cyber crimes and developed states should assist them in developing and institutionalizing strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cyber security at domestic level. Bilateral and multinational cooperation between AALCO Member States in this regard could focus on dialogue and coordination in dealing with cyber threats.

ANNEX

SECRETARIAT'S DRAFT
AALCO/RES/DFT/54/S17
17 APRIL 2015

RESOLUTION ON "INTERNATIONAL LAW IN CYBERSPACE"

(Deliberated)

The Asian-African Legal Consultative Organization in its Fifty-Fourth Session,

Having considered the Secretariat Document No. AALCO/54/BEIJING/2015/SD/S17 prepared by the AALCO Secretariat,

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

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

Realizing the need to democratize the governance of the Internet in pursuance of equity and bridging the "digital divide" prevalent in developing States,

Acknowledging the importance of balancing sovereign rights of the States and fundamental freedoms of speech and expression of its citizens in cyberspace,

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

1. **Urges** the Member States to respect international law, in particular the UN Charter and other relevant instruments related to state conduct in cyberspace;

2. **Encourages** Member States to actively participate in the relevant regional and global forums deliberating on the governance of cyberspace;

3. **Decides** to establish an open-ended working group on international law in cyberspace to further discuss the matter through meetings or workshops to be cosponsored with Governments of the Member States or relevant international organizations;

4. **Decides** to place the item on the Provisional Agenda of the Fifty-Fifth Annual Session.