RELEVANCE OF INTERNATIONAL LAW IN COMBATING CYBERCRIMES: CURRENT ISSUES AND AALCO'S APPROACH

Prof. Dr. Kennedy Gastorn*

Secretary General of Asian-African Legal Consultative Organization (AALCO)

Presentation at the 4th World Internet Conference, Wuzhen Summit, on the Session on "International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes", 4th December 2017, Wuzhen, China

Outline

* Any views contained or expressed in this article are those of the author and are neither intended to, nor do they, necessarily represent the views of any other individual or body associated with AALCO or its Member States. The author is grateful for the assistance received from Amrita Chakravorty and Kiran Mohan, Legal Officers, AALCO.

1. Introduction

It needs no technical expertise to appreciate the fact that information security issues are inherently and unavoidably global in nature. And cybercrime is an example of one of the fastest growing transnational crimes. However, the means available to investigate and prosecute such cyber-related crimes are mostly national in scope.

Cybercrimes raise several challenges for traditional criminal law and the criminal justice system in general. First and foremost, the nomenclature 'cybercrime' itself covers a wide range of offences – including offences against the confidentiality, integrity and availability of data and information systems, computer-related offences, content-related offences, such as child pornography and acts of a racist and xenophobic nature, as also the offences related to the infringement of copyright.

The second challenge is that Information and Communication Technology (ICT) is complex and frequently unfamiliar to the traditional criminal justice world. Dealing with crimes involving these devices requires well-trained personnel in the investigation phase, during prosecution, and in courts. Technological and computer knowledge are somewhat alien to law enforcement and legal cultures.

The third main challenge associated with cybercrimes is regarding sovereignty issues, as they take place in virtual environments. Owing to the global and unique nature of cybercrimes, inconsistencies among criminal justice systems is a major hindrance in the repression of the phenomena.

In many countries, the explosion in global connectivity has come at a time of economic and demographic transformations, with rising income disparities, tightened private sector spending and reduced financial liquidity. Also, commission of cybercrimes no longer requires complex skills or techniques. In the developing country context in particular, sub-cultures of young men engaged in computer-related financial fraud have emerged, many of whom begin involvement in

cybercrime in late teenage years.[1] In fact, more than 80 per cent of cybercrimes are estimated to originate in some form of organized activity and often has an international dimension, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information.[2]

Compared to conventional crimes, laws addressing cybercrimes need to contain more advanced investigative measures, jurisdiction related rules and rules relating to electronic evidence, and hence, there is a requirement for international cooperation. A transnational dimension to a cybercrime offence arises where an element or substantial effect of the offence is in another territory, or where part of the *modus operandi* of the offence is in another territory.

The World Internet Conference (WIC), with its scale of participation and the relevance of subjects discussed, is one of the most influential and anticipated annual events on cyberspace. Its Fourth Edition at Wuzhen, under the theme of "Developing Digital Economy for Openness and Shared Benefits — Building a Community of Common Future in Cyberspace", provides an apt forum to discuss the ways and means to further international cooperation to effectively combat cybercrimes as cyber security is an essential precondition to fully realize the potential of a global digital economy based on equitable and transparent sharing of resources.

2. International Framework

The proliferation of transnational cybercrimes is compounded by the absence of effective global norms and cooperation mechanisms to prosecute and punish perpetrators. Reflecting such concerns of the international community, the UN General Assembly has adopted a series of resolutions emphasizing that 'the dissemination and the use of information technologies and means affect the interest of the entire international community that the criminal misuse of

[1] "Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector", UNODC/CCPCJ/EG 4/2013/2, (23 January, 2013).
[2] UNODC Study, Ibid., <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

information technologies may have a grave impact on all States….and these technologies can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security'.[3] The UN General Assembly also actively supported the cause of curbing cyber-crimes at the World Summit on Information Society (WSIS) which were held in two phases in Geneva in 2003 and Tunis in 2005. At WSIS, Heads of States and world leaders entrusted the International Telecommunication Union (ITU) to be the Facilitator of Action Line C5, 'Building confidence and security in the use of ICTs', in response to which ITU launched, in 2007, the Global Cybersecurity Agenda (GCA), as a framework for international cooperation in this area.[4]

International legal measures play an important role in the prevention and combating of cybercrime. The last decade has, therefore, seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. These include binding and non-binding instruments. A number of the instruments – notably the Council of Europe Conventions, the Shanghai Cooperation Organization Agreement, and the League of Arab States Convention – are express agreements and are intended to create legal obligations among the State parties. A few other instruments such as the Commonwealth Model Law, the Common Market for eastern and Southern Africa (COMESA) Draft Model Bill, the League of Arab States Model Law, and the ITU/CARICOM/CTU Model Legislative Texts – are not intended to create legal obligations for States. Rather, they are designed to serve as models for development of national legislative provisions.

Therefore, as we have seen non-binding instruments do have a significant influence at the global or regional level when States may choose to align their national laws with model approaches. In addition to formal membership and implementation, multilateral cybercrime instruments have influenced national laws indirectly, through use as a model by non-State parties, or via the influence of legislation of State parties. It is also important to note that significant cross-fertilization has occurred among these instruments. The basic concepts developed in the Council of Europe Cybercrime Convention, for example, are also found in many other instruments.

[3] *See* e.g., the preambular paragraphs of Resolutions A/RES/55/28 of 20 November 2000; A/RES/60/45 of December 2005; A/RES/64/25 of 2 December 2009.
[4] ITU Cybersecurity Activities, available at: <http://www.itu.int/en/action/cybersecurity/Pages/default.aspx>.

United Nations entities, such as ITU, have also had some involvement in the development of instruments in the African context, including the Draft African Union Convention.[5]

Evidently, regional instruments dominate the existing regime of international law addressing cybercrimes.

2.1. The Budapest Convention

As the Internet exploded across the globe in the mid-1990s, the Council of Europe was the first intergovernmental treaty organization to deal with cybercrimes, particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security; and began the work of drafting a convention as early as 1996 that would not only deal with criminal substantive law matters, but also with criminal procedural questions as well as with international criminal law procedures and agreements. After four years of negotiations the Budapest Convention on cybercrimes was finalized in 2001, and came into force in 2004. The Convention not only assisted in the convergence, consistency and compatibility of cybercrime legislation between infrastructure countries but also guided developing nations towards best practices in writing their own cybercrime legislation.[6]

It has been widely recognized as a decisive document on international best practice. Most model legislations and attempts at drafting a new international instrument on cybercrime have in fact relied on the principles expounded in this Convention. Notably, AALCO Member States like Egypt, Nigeria and Pakistan have used the Convention as a model and drafted parts of their legislation in accordance with it without formally acceding to it. The Convention on Cybercrime was followed by the First Additional Protocol to the Convention on Cybercrime which came into force in 2006.[7] The States ratifying the Additional Protocol are required to criminalize the dissemination of racist and xenophobic material through cyberspace.

---

[5] See International Telecommunication Union, "Understanding Cybercrime: Phenomena, Challenges and Legal Response", (2012), p. 29.

[6] Pakistan, for instance, modeled its legislations based on the Convention. The Convention served as an effective model for international cooperation in combating cybercrimes. See Zahid Jamil, "Global Fight against Cybercrime: Undoing the Paralysis", *Georgetown Journal of International Affairs*, (22 March, 2013).

[7] Available at: <https://ccdcoe.org/sites/default/files/documents/CoE-030128-AdditionalProtocol.pdf>.

Nevertheless, the Convention faced and continues to face opposition from certain quarters that traditionally tend to promote a greater role for the regulation of the Internet by UN bodies. Further, there are arguments that there are inadequacies in the Convention that reduce its effectiveness. After all, cybercrime is an area of crime that is constantly changing. In the 1990s, when the Budapest Convention was developed, terrorist use of the Internet, botnet attacks and phishing 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.[8]

Another frequently criticized aspect of the Convention is the inadequate representation of developing countries in the drafting process. Despite the transnational dimension of cybercrime, its impact in the different regions of the world is different. This is especially relevant for developing countries. Some States declined to adopt it citing that they did not participate in its drafting.[9]

There are views, however, even amongst the AALCO Member States, which contradicts the criticism that the Convention was designed solely by and for developed countries. The said view is based on the premise that the Convention is based on the universal needs of the practitioners working on cybercrime investigation and prosecution around the globe, and can be applied in any State as the universal standard of cybercrime investigation and prosecution.[10]

On the other hand such concerns have also been raised in AALCO meetings that relate to the redundancy of the Convention as it was negotiated and adopted more than 12 years ago. A counter view was that the Convention employs technologically-neutral language in defining

[8] See generally Amelie Weber, "The Council of Europe's Convention on Cybercrime", *Berkeley Technology Law Journal*, Vol. 18 (2003).
[9] See Anja Kovacs, "India and the Budapest Convention", available at < https://internetdemocracy.in/reports/india-and-the-budapest-convention-to-sign-or-not-considerations-for-indian-stakeholders/>.
[10]See Statements of Japan, Agenda Item: International Law in Cyberspace, Fifty-Fourth Annual Session of AALCO, Beijing, 2015; New Delhi, 2016.

criminal acts and criminal justice procedures and, therefore can be applied to novel technologies and newest developments in cyberspace.

Therefore, the reality today is that some States continue to support negotiating a comprehensive international convention on combating cybercrime under the aegis of the United Nations,[11] while others caution against duplication of efforts, creating something very similar to the Budapest Convention.[12] Such differences do warrant a wider and deeper series of discussions and consultations on cybercrime issues not only amongst AALCO Member States but also between the Member States and other States and organizations.

2.2 **Agreement on Cooperation in the Field of Ensuring International Information Security and the International Code of Conduct for Information Security**

The Shanghai Cooperation Organization (SCO) is a Eurasian security organization, originally comprising of six Member States (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan), and established in 2001 for the purposes of political, military and economic cooperation. A particular focus of the Organization has been on fighting the 'three evil forces' of terrorism, separatism and extremism. In 2009, an Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security (Yekaterinburg, 16 June 2009) was concluded.

India, Pakistan, Mongolia and Iran have had observer status, and Belarus and Sri Lanka have been the two dialogue partners within the SCO. India and Pakistan were formally inducted as the newest members of the Organization on 8 September, 2017, in the first-ever expansion of the six-member group.

International information security has figured prominently on SCO's agenda, which has seriously been concerned about threats arising from the cyberspace, as well as the West dominance of the

[11] See Statement of People's Republic of China and Islamic Republic of Iran, Agenda Item: International Law in Cyberspace, Fifty-Fourth Annual Session of AALCO, Beijing, 2015.
[12] See Statement of Malaysia, Agenda Item: International Law in Cyberspace, Fifty-Fourth Annual Session of AALCO, Beijing, 2015.

Internet. The SCO Agreement in the Field of International Information Security underlined the "digital divide" amongst States. It was made out of the increasing fear that the chances of participation of developing nations in international IT collaborations was dwindling. The SCO economies are interested in controlling information that is likely to provoke what they call the 'three evils': terrorism, extremism and separatism. They consider it important to prevent nations from using their technologies to disrupt economic, social and political stability and security of other sovereign nations. Western nations, on the other hand, by and large maintain that too much State control may severely hamper cyberspace freedom.

The International Code of Conduct for Information Security (the "Code") was submitted for consideration to the UN General Assembly in September 2011 by the Member States of the SCO — China, Russia, Tajikistan, and Uzbekistan. In January 2015 an updated version of the Code was offered by all six Member States of the Shanghai Cooperation Organization (SCO) — China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.

The initial draft, proposed in 2011, sought to identify the rights and responsibilities of States in the information space by, *inter alia*, calling on them:

- to comply with the Charter of the UN by highlighting the respect for sovereignty and territorial integrity;
- not to use ICT for hostile activities and aggression and not to proliferate information weapons or related technologies;
- to cooperate in combating criminal and terrorist activities that use ICT;
- to promote the establishment of a democratic and multilateral internet management system; and
- to promote the 'important role of the United Nations in formulating international norms.[13]

It is alleged that the original proposal could not garner much global support, owing to certain contentious aspects - for example, the Code emphasizes that a 'multilateral' (intergovernmental)

[13] "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General", A/66/359, (14 September, 2011).

system for Internet governance should be developed – a construct inconsistent with the current 'multi-stakeholder' system that is viewed as being dominated by the US.[14]

The revised draft has carried out some noticeable changes, such as the omission of the somewhat controversial term 'information weapon'.[15] The new wording is consistently very broad, allowing that any use of 'information and communications technologies' could be classified as inconsistent with 'maintaining international peace and security'. The new Code of Conduct also features an entirely new section (Section 7) including a general principle that is gaining wide support globally by calling on States to recognize 'that the rights of an individual in the offline environment must also be protected in the online environment', subject to certain restrictions, based on the International Covenant on Civil and Political Rights.

The International Code of Conduct for information security is intended to be an open and sustained process of building international consensus. It is further hoped that the UN GGE on information security would be made full use of, as an important platform to deepen mutual understanding and explore the international norms and rules. Lastly, the Code aspires that governments should play a major role in the area of information and cyber security. At the national level, governments should lead all stakeholders, including private sectors, in addressing the security challenges and strengthening the legislation and institutional capacity building. At the international level, States should carry out effective cooperation in preventing and combating cybercrimes and cyber terrorism, protection of critical information infrastructure, as well as the maintenance of stable and secure functioning of information and communication systems.[16]

[14] "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?",*Incyder News*, (10 February, 2015), available at: <https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html>.

[15] "Each State voluntarily subscribing to the code pledges: …b) Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies", International Code of Conduct for Information Security.

[16]"An International Code of Conduct for Information Security: China's Perspective on Building a Peaceful, Secure, Open, and Cooperative Cyberspace", (10 February, 2014, Geneva).

2.3 Association of Southeast Asian Nations (ASEAN)

Comprising ten Southeast Asian States, the ASEAN was established in 1967 to promote intergovernmental cooperation and economic integration. A lot of its Members are also the Member States of AALCO.

ASEAN Member States cooperate and share best practices on ICT and business processes at the forum of Telecommunications and IT Ministers Meeting (TELMIN). The ASEAN further engages with China, Japan, Republic of Korea, EU, and the ITU to implement their respective annual ICT work plans and joint activities. The ASEAN Chiefs of Police (ASEANAPOL) meet regularly to discuss issues of cybercrime laws. The ASEANAPOL is also in the process of establishing a partnership with the INTERPOL's Global Complex (IGC), in Singapore.

Cyber-security related initiatives at ASEAN emerged as a reaction to the pervasive and disruptive nature of regional cybercrimes. The Master Plan on ASEAN Connectivity was adopted by the ASEAN Leaders at the 17th ASEAN Summit in 2010. The Master Plan serves to achieve a bold and long-term strategy to improve the region's physical, institutional and people-to-people connections. The 'physical connectivity' component of the Plan includes transport; information and communications technology (ICT); and energy. This Plan under strategy 6 hopes to accelerate the development of ICT infrastructure and services in each of the ASEAN Member States. The following is the key action to be taken: "(iv) Promote network integrity and information security, data protection and Computer Emergency Response Team (CERT) cooperation by developing common frameworks and establishing common minimum standards where appropriate, to ensure a level of preparedness and integrity of networks across ASEAN by 2015".[17]

The Master Plan on ASEAN Connectivity 2025 adopted in 2016 seeks to add value by complementing and synergizing the ASEAN Community Blueprints 2025. The study in this regard on the establishment of the ASEAN Broadband Corridor has been completed and endorsed in March 2013. This has provided the framework to identify key drivers for broadband

[17] "ASEAN's Perspective on Cyber security", ASEAN-India Conference on Cyber Security in New Delhi, India, (Association of South East Asian Nations), (19 January, 2015).

rollout and recommendations on specific government initiatives to influence each key driver of broadband rollout. The ASEAN Internet Exchange Network (AIX) project was concluded with a report on the status of peer-to-peer connections between Internet Exchange providers across ASEAN Member States and a recommendation to encourage private sector operators to establish more peer-to-peer connections with their ASEAN counterparts across the borders. The procurement of the implementer of the feasibility study on 'Establishing an ASEAN Single Telecommunications Market' is currently in process.[18]The strategic objectives for the same are as follows: a) supporting the adoption of technology by micro, small and medium enterprises (MSMEs); b) supporting financial access through digital technologies; c) improve open data use in ASEAN Member States; and d) supporting enhanced data management in ASEAN Member States.[19]

2.4 The Arab Convention on Combating Information Technology Offences, 2010

The League of Arab States instrument – The Arab Convention on Combating Information Technology Offences was enacted in 2010 with the aim of enhancing cooperation between Arab countries 'to combat information technology offences threatening their security, interests and the safety of their communities' and enabling parties to 'adopt a common criminal policy aimed at protecting the Arab society against information technology offences'. The Arab Convention has been signed by 18 Arab countries, including all six Gulf Cooperation Council Members.

Talking of cyber-crime prevention within the Gulf Cooperation Council, however, analysts on the subject are of the opinion that intra-GCC cooperation on combating cybercrime more or less relies on bilateral relationships and informal channels, such as police-to-police or agency-to-agency cooperation.[20]While these mechanisms are useful, they are insufficient for an effective regime: they place limitations on investigative actions, lack a common approach, and have to operate within multiple law enforcement networks. Informal mechanisms normally serve as a precursor to formal requests for Mutual Legal Assistance Treaties (MLATs), which are

[18]"Master plan on ASEAN Connectivity 2025", *The ASEAN Secretariat, Jakarta*, (2016), p. 20.
[19]Ibid. p. 50.
[20] Joyce Hakmeh, "Cybercrime and the Digital Economy in the GCC Countries", *International Security Department, Chatham House*, (June, 2017), p. 12.

'agreements between governments that facilitate the exchange of information relevant to an investigation happening in at least one of those countries.'[21]

2.5 The African Union Convention on Cyber security and Personal Data Protection

To address the challenges posed by criminal activities committed over ICT networks in a manner that is relevant to regional and continental specificities and in response to the need for harmonized legislation in the field of cyber security and personal data protection across the African nations, the 23rd Assembly of Heads of State and Government adopted in June 2014 the 'African Union Convention on Cyber Security and Personal Data Protection', also known as the 'Malabo Convention'.

The Malabo Convention seeks the establishment of a comprehensive continental legal framework that sets broad guidelines for electronic transactions, personal data protection as well as cyber security to prevent cybercrime in the African cyber ecosystem. It embodies the existing commitments of African Union (AU) Member States at sub-regional, regional and international levels to build an information society that respects cultural values and beliefs of the African Nations, and guarantees a high level of legal and technological security to ensure respect of privacy and freedoms online while enhancing the promotion and development of Information and Communication Technologies (ICT) in the AU Member States. The Convention sets out the essential security principles for establishing a credible digital environment with a view to reduce the risks of cybercrime and abuse of personal data.[22]

To facilitate its implementation by African countries, the African Union Commission in collaboration with Internet Society developed guidelines on internet infrastructure security for Africa. The Guidelines emphasize the importance of the multi-stakeholder model and the need for collaborative security in protecting internet infrastructure with particular focus on essential principles of internet infrastructure security in Africa. These include, most notably, raising

[21]UNODC (2013), *Comprehensive Study on Cybercrime*, Draft–February 2013.
[22]Dawit Bekele, "The African Union Commission and Internet Society Support Internet Infrastructure Security in Africa", Global Forum on Cyber Expertise, (31 May, 2017).

awareness at different levels, responsibility, cooperation, and adherence of all the concerned actors to fundamental rights and internet properties.[23]

The convention deserves praise for prioritizing the need for African States to address the problem of cybercrime and tackle deficiencies in their cyber security. However, it is unclear whether the concerns that had delayed the convention's consideration in January 2014 have been adequately addressed. There are further concerns that the scope of the convention is overly ambitious and too cumbersome, as it deals with many areas of electronic activity beyond cybercrime. The few African states that have enacted cybercrime laws, including Cameroon, Kenya, Mauritius, South Africa and Zambia, will have to engage in an arduous process to reconcile differences between their laws and the convention's requirements. The vast majority of African States without cybercrime laws will have to draft cybercrime legislation from scratch. This process will be difficult given the lack of awareness about cybercrime in Africa, the inherent complexities of the problem and deficiencies in capacity across the continent.[24]

The AU convention faces another challenge in that it joins a crowded field of bilateral and multilateral cybercrime conventions, draft frameworks and model laws. In Africa, regional economic communities (RECs) have developed the following conventions (a) East African Community (EAC) Draft Legal Framework for Cyberlaws (2008), (b) Economic Community of West African States (ECOWAS) Draft Directive on Fighting Cybercrime (2009), (c) Common Market for Eastern and Southern Africa (COMESA) Cyber Security Draft Model Bill (2011), and (d) Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (2012)

Regardless of their form, instruments developed by RECs have had difficulty gaining support in their respective regions. Whether the AU convention will have more success across the continent

[23] Ibid.
[24] According to a cybercrime study by the United Nations Office on Drugs and Crime (UNODC), every country in Africa that responded to its questionnaire indicated a need for technical assistance. See UNODC, *Comprehensive study on cybercrime: draft – February 2013*, February 2013, 178, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. ElevenAfrican countries responded to the UNODC cybercrime questionnaire. See generally, Eric Tamarkin, "AU's Cyber Crime Response: A Positive Start but Substantive Challenges Ahead", *Institute for Security Studies*, Policy Brief 73 (January, 2015).

is yet to be determined. AU hence continues to face significant hurdles in convincing all African States to ratify the convention and implement its provisions. Furthermore, some of the convention's cybercrime provisions remain controversial and it fails to tackle the fact that fighting cybercrime requires international cooperation reaching beyond Africa's geographical borders.[25]

2.6 United Nations

The United Nations (UN) has been working for over a decade to eliminate the existing differences in various regional and sub-regional cyber-laws and create a mechanism to ensure the security and stability of cyberspace. The UN First Committee on Disarmament and International Security which deals with disarmament, global challenges and threats to peace has been discussing the issue of information security since 1998, when the Russian Federation introduced a draft resolution on "Developments in the field of information and telecommunications in the context of international security" in the General Assembly (GA). Amongst the substantial work at the UN has also been the constitution of Group of Governmental Experts (UN GGEs) (thrice). One of the primary issues of differences between States in these Groups, however, has been on the question of the impact of developments in information and communications technologies (ICTs) on national security and military affairs.

Despite near universal support for international action against cybercrime, there is currently no binding global cybercrime agreement; even though a lot of important work has been done till date under the premises of the UN. Firstly, the UN Resolutions on Combating the Criminal Misuse of Information Technologies raised many issues.[26] However, none of these measures were binding, with Member States invited to take them into account in developing their own efforts to combat the criminal misuse of information technologies. Then out of the first phase of the World Summit on the Information Society, held in Geneva in 2003 came the *Geneva*

[25] Eric Tamarkin, "AU's Cyber Crime Response: A Positive Start but Substantive Challenges Ahead", *Institute for Security Studies*, Policy Brief 73 (January, 2015). See also, Mailyn Fidler, "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity", *Council on Foreign Relations*, (22 June, 2015).
[26] See for example, *Combating Criminal Misuse No 1*, UN Doc A/RES/55/63; *Combating Criminal Misuse No 2*, UN Doc A/RES/56/121.

Declaration of Principles and the *Geneva Plan of Action*.[27]The latter included action line C5, 'Building Confidence and Security in the use of ICTs', Article 12(b) of which contained a number of measures that governments should take, in cooperation with the private sector, to 'prevent, detect and respond to cyber-crime and misuse of ICTs'. The second phase held in 2005 produced the *Tunis Agenda for the Information Society*. In the context of legislative reform, this called upon governments 'to develop necessary legislation for the investigation and prosecution of cybercrime' taking into account existing frameworks and regional initiatives 'including, but not limited to the Budapest Convention.[28]

In 2007 the ITU, which is responsible for facilitating action line C5, launched its Global Cyber-security Agenda (GCA).[29]The GCA is divided into five pillars/work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. Yet the GCA does not pursue a binding global initiative. The first of the seven strategic goals 'calls for the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures'.[30]

Even though the Internet remains borderless from a technological point of view, many Member States of the UN are of the view that a completely open and minimalist Internet could lead to significant security issues. On September 12, 2011, the permanent representatives of people's Republic of China, Russia, Tajikistan and Uzbekistan to the United Nations submitted a letter jointly to the United Nations Secretary-General Ban Ki-moon, asking him to distribute the International Code of Conduct for Information Security drafted by their countries as a formal document of the 66th session the General Assembly and called upon countries to further discuss the document within the framework of the United Nations so as to reach consensus on the

[27]World Summit on the Information Society, 'Plan of Action' (Document No WSIS-03/GENEVA/DOC/5-E, International Telecommunication Union, 12 December 2003) ('*Geneva Plan of Action*').
[28] World Summit on the Information Society, 'Tunis Agenda for the Information Society' (Document No WSIS-05/TUNIS/DOC/6(Rev. 1)-E, International Telecommunication Union, 18 November 2005).
[29] Available at: <http://www.cybersecuritygateway.org/pdf/new-gca-brochure.pdf>.
[30] See *Global Cyber Security Agenda*. Also see generally, Jonathan Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization", *Monash University Law Review*, (Vol. 40(3)), (2013).

international norms and rules standardizing the behavior of countries concerning information and cyberspace at an early date.[31]

The International Code of Conduct for Information Security, as mentioned earlier, raises a series of basic principles of maintaining information and network security which cover the political, military, economic, social, cultural, technical and other aspects. The principles stipulate that countries shall not use such information and telecom technologies as the network to conduct hostile behaviors and acts of aggression or to threaten international peace and security, and stress that countries have the rights and obligations to protect their information and cyberspace as well as key information and network infrastructure from threats, interference and sabotage attacks. They advocate establishing a multilateral, transparent and democratic international Internet governance mechanism, fully respecting the rights and freedom of information and cyberspace with the premise of observing laws, helping developing countries develop the information and network technologies and cooperating on fighting cyber-crimes.[32]

This International Code of Conduct for Information Security notably, calls upon all its signatories to comply with the UN Charter and universally recognized norms governing international relations, which enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all states, respect for human rights and fundamental freedoms, as well as respect for diversity of history, culture and social systems of all countries.[33]Hence, even in the matters of cyber-security, differences amongst the two main factions of States, advocating for and against an open and minimalist Internet (including one faction trying to contain economic espionage and criminal activity in cyberspace, and the other looking at broader rules that would restrict a State's ability to use cyberspace for offensive purposes) – has to a great extent prevented the adoption of a universal legal regime in this regard.

[31] "China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations",
(13 September, 2011), available at: <http://nz.chineseembassy.org/eng/zgyw/t858978.htm>.
[32]Ibid.
[33]Ibid.

3 Deliberations at AALCO

In the past decade many AALCO Member States increasingly recognized the need for comprehensive legislations to combat cybercrimes.[34]In tandem with national developments, AALCO Member States have joined various international and regional instruments aimed at countering the proliferation of cybercrimes and improving international cooperation for the harmonization of cyber-laws. However, differences between Member States regarding the mechanism for such harmonization still continue to persist. While some States advocate for the formulation of a comprehensive global convention, others are in favor of harmonizing domestic laws to the standards of existing international instruments.[35] Further, as already discussed, a few AALCO Member States have not been in favor of a more universal ratification of the Budapest Convention.

Recognizing *inter alia* the importance of intergovernmental deliberation to enhance cooperation in combating cybercrimes, People's Republic of China, in accordance with AALCO Statutory Rules, proposed "International Law in Cyberspace" as an agenda item to be deliberated at the Fifty-Third Annual Session of AALCO held in Tehran in 2014 and it was accepted by consensus. The Agenda Item was thereafter discussed at the Fifty-Fourth, Fifty-Fifth and fifty-Sixth Annual Sessions, in 2015, 2016 and 2017 respectively.

The resolution on the agenda item adopted in the 2015 AALCO Annual Session directed the Secretariat to study this subject based on deliberation and progress made in the UN framework and other forums, with special attention to international law pertaining to State Sovereignty in cyberspace, 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. The "Special Study" published by the Secretariat in 2017 has an exclusive chapter detailing the hitherto international efforts in addressing the menace of transnational cybercrime.

[34] For example, the Iranian Cyber Crimes Act of 2009 has provisions for preventing illegal infiltration.

[35]See for example, statements of Japan and People's Republic of China, Agenda Item: International Law in Cyberspace, Fifty Fourth Annual Session of AALCO, Beijing, 2015; Fifty Fifth Annual Session of AALCO, New Delhi, 2016; and Fifty Sixth Annual Session of AALCO, Nairobi, 2017.

Further, an Open-ended Working Group on International Law in Cyberspace was constituted in 2015 which met for the first time at the Fifty-Fifth Annual Session in 2016. The second meeting was held at the AALCO Headquarters in New Delhi in February, 2017. In that meeting, Dr. Huang Zhixiong, Rapporteur of the Working Group, remarked that regional and global instruments can certainly co-exist, and AALCO Member States should consider drafting Model Rules in this regard. Further, one of the Member States stressed upon the need to have a Model Law in place as regards rules of international law in combating cybercrimes, keeping in mind the best interest of all Member States.

AALCO will continue its deliberations and discussions in the future sessions and will chalk out a detailed plan in the next meeting of the Working group as regards the future direction of its work in pursuit of a comprehensive and equitable development of international norms governing cyberspace.

4 Concluding Remarks: Importance of Harmonization

It is evident that even though the international community recognizes full well that the harmonization of laws and facilitation of international cooperation is essential to achieving global cyber security, till date it has not been able to finalize a universal comprehensive code to combat cyber-crimes, mainly due to the differences amongst nations as to the approach to such harmonization. Forms of international cooperation today include extradition, mutual legal assistance, mutual recognition of foreign judgments and informal police-to-police cooperation. Due to the volatile nature of electronic evidence, however, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as preservation of computer data.

The mechanism whereby such harmonization can be achieved remains contested. Nevertheless, to see harmonization as a destination is unrealistic, as it is a process. As the technology evolves and changes so too our responses will need to evolve and change. Rather than focusing on differences as an impediment to harmonization, the focus should be on how those differences

may be resolved in working towards the common goal of effective international cooperation against a global challenge.

Each country will have to determine what it considers necessary to effectively combat cybercrime, by looking into national, regional and international standards in enacting laws that best suit its national circumstances. Nonetheless, a global agreement provides a crucial benchmark against which such efforts can be measured, providing an internationally recognized framework for the harmonization of cybercrime laws. For those countries that are unable to, or choose not to ratify, it would provide an important model against which their own laws can be compared. The UNODC and Council of Europe, as well as other regional and national initiatives play an extremely valuable role in information sharing and capacity building. In this way differences and diversities become drivers of change – shifting the focus to what needs to be achieved rather than how difficult it will be.

However, despite the existence of many international instruments, a lack of common approach, including within these multilateral cybercrime instruments, means that requests for actions, such as expedited preservation of data outside of those countries with international obligations to ensure such a facility and to make it available upon request, may not be easily fulfilled. Hence, it is not wrong to state that the current divergences in the scope of cooperation provisions in multilateral and bilateral instruments, a lack of response time obligation, a lack of agreement on permissible direct access to extraterritorial data, multiple informal law enforcement networks, and variance in cooperation safeguards, represent significant challenges to effective international cooperation regarding cybercrimes.

AALCO, as a multilateral forum representing such divergent interests and positions on the topic, holds immense potential for its Member States to be used as a platform to further deliberate on outstanding issues that come in the way of effective cooperation mechanisms.