XI. VERBATIM RECORD OF THE SPECIAL HALF-DAY MEETING ON "INTERNATIONAL LAW IN CYBERSPACE"

XI. VERBATIM RECORD OF THE SPECIAL HALF-DAY MEETING ON "INTERNATIONAL LAW IN CYBERSPACE" HELD ON WEDNESDAY, 15 APRIL 2015 AT 9.30 AM

H.E. Liu Zhenmin, Vice Minister of Foreign Affairs of the People's Republic of China, and President of the Fifty Fourth Session AALCO Annual Session is in the Chair.

President: Good morning distinguished delegates and dear colleagues. Today we enter our third day of meetings and I hope you have all rested well from last night. I welcome you all to the "Half-Day Special Meeting on International Law in Cyberspace". As you are aware, the development of internet technology has brought to people around the world immense economic benefits and, at the same time, it has also brought unprecedented challenges without geographical limits. In 2013, the report of a group of governmental experts of the UN affirmed the applicability of international law, and in particular the UN Charter, which is essential to maintaining peace and stability, and promoting an open, secure, peaceful, and accessible ICT environment.

However, there is still limited consensus on how international law might apply in cyberspace, or how to prevent the risky trend of militarization and ensure peace in cyberspace through international law. I feel this meeting presents to us an important opportunity to try and identify ways and means of doing so. The issue we are discussing is a new issue to all international forums, but I think the AALCO Annual Session provides a good opportunity for Afro-Asian countries to have a debate on the issue.

To begin this meeting I invite the Deputy Secretary General, Mr. Feng Qinghu to make his introductory remarks on the topic. Mr. Feng, you have the floor.

Mr. Feng Qinghu, Deputy Secretary General of AALCO: Thank you, Your Excellency, Mr. President. Respected Panelists, Excellencies, Distinguished Delegates, Ladies and Gentlemen;

This agenda item is one of the latest additions to our programme. It was People's Republic of China that proposed "International Law in Cyberspace" as an agenda item to be deliberated at the previous Annual Session of AALCO, held in Teheran in 2014, and it was accepted by consensus. Cyberspace is the newest realm of human interaction and its unique structure and framework poses considerable challenges to nation States and the international community as a whole. These challenges include, *inter alia*: 1) disagreement over a universally accepted structure of internet governance and associated issues including State sovereignty in regulating the internet within its jurisdiction; 2) articulation of rules relating to State and non-State conduct during cyber-warfare; and, 3) burgeoning transnational cybercrimes and the need for multilateral treaties to effectively prevent its escalation. The report of the Secretariat focusing on this area is contained in AALCO Report AALCO/54/BEIJING/2015/SD/S 17.

Excellencies, the existing internet governance regime has often been portrayed as a non-hierarchical, 'multi-stakeholder-model', which consists of governments, private companies and non-governmental organizations. However, in practice this 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 the International Telecommunication Union (ITU) at its center. This appears to be a distant possibility, as is evident from the result of ITU's recently concluded Plenipotentiary Conference 2014, wherein the position of the developed nations prevailed.

Excellencies, an associated issue that was stressed in the last Annual Session is State sovereignty in cyberspace. The arguments favouring greater State control over internet governance primarily hinge on the extension of State sovereignty to cyberspace. 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, it is significant to point out here, as embodied in Article 19 of the Universal Declaration of Human Rights, that freedom of expression and information must be promoted without exception. The exercise of sovereignty by any State must be subjected to this right.

Excellencies, cyberspace has become the "fifth domain" of war with militaries across the globe increasingly becoming reliant on cyber networks and computer-aided warfare. The articulation of traditional rules of war, both on the use of force (*jus ad bellum*) and International Humanitarian Law (*jus in bello*), applicable to cyberspace is a prime concern. Tallinn Manual on the International Law Applicable to Cyber Warfare may serve as an important reference in this regard.

Further, cyber espionage factors in as a critical concern with respect to cyber security. Large-scale snooping on the foreign missions and other activities of many nations has been reported in the recent past. In this context, it is to be emphasized that the Vienna Convention on Diplomatic Relations reaffirms the inviolability of diplomatic correspondence and it equally applies to cyberspace as well.

Lastly, 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.[1] Given the low 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. In fact, the Convention on Cyber Crimes, which is also called as Budapest Convention, is the only existing multilateral treaty that specifically addresses computer related crimes. However, its provisions do not adequately address various new threats such as terrorist use of the internet, botnet attacks and phishing.

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

Excellencies, it is roughly in this context that we are deliberating this agenda item. It is our firm belief that today's deliberations provide us a good opportunity to discuss these issues which would lead to finding solutions to the challenges posed by transnational activities in cyberspace. Thank you.

President: I thank Mr. Feng, the Deputy Secretary General of AALCO, for his introductory statement. Dear colleagues, you may have noticed that for today's discussion we have invited two panelists. On my left is Mr. Richard Desgange, the Regional Legal Advisor for ICRC. To my far right is Mr. Fan Zhijong from *Huawei*. Let me first give the floor to Mr. Fan Zhijong to provide us with some background knowledge about cyberspace. Mr. Fan, you have the floor.

Mr. Fan Zhijong, Representative of *Huawei*: Thank you, Your Excellency. Ladies and gentlemen, good morning. My name is Fan Zhijong, and I am the Vice-President of Intellectual Property Strategy at *Huawei*. The internet is changing our life, and the internet itself is also changing. So, the way it is changing our life is changing. Engineers describe change over change as acceleration. Today we are going to look at the past, present, and future of the internet, and navigate through the economic and policy implications of the accelerated changing.

I want to begin with the case study of a Chinese company called *Taobao*, a client of *Huawei*. *Taobao* is a leading e-commerce company in China for online shopping. On 11 November 2014, $3.9 billion were spent by consumers using *Taobao*'s mobile phone application. That's 460% up from 2013. The question is, why has there been such a dramatic growth of almost five-fold in merely a year? Has anything changed?

The secret is here: In December 2013, the Ministry for Industry and Information Technology issued licenses to all three mobile operators in China allowing them to operate Fourth Generation (4G) wireless networks. The main difference between 4G and 3G (third generation) is about ten times in speed. Think of downloading a movie; a full-length high-quality movie will take 70 minutes using 3G under the best network conditions, but it would only take 7 minutes using 4G. The faster 4G networks led to the thriving of mobile internet applications that dramatically changed the Chinese peoples' lives in 2014. But that was just the beginning. Engineers working at *Huawei* and many other companies are working hard to bring Fifth Generation (5G) networks to life within ten years. The 5G network will be 66 times faster than 4G, and will open doors to a totally new world.

But before we look at the case of present-times and dive into the future, let us take some time to review our case study of *Taobao* from an economic perspective. As policy makers, you should be interested in seeing those figures. By 2013, *Taobao* and its online merchants created 12 million jobs; greater than the population of Tokyo. In case your economic advisor may say that is merely a transitioning from real shops to online shops, the World Bank Report provided its estimation that every 10% of broadband penetration will lead to 1.3% growth of GDP and 2-3% of new jobs, and that is GDP growth not at the cost of our precious environment. 10% of broadband penetration will also lead to 5% reduction of CO2 emission, and perhaps most importantly 15-fold increase in innovation efficiency. This innovation will lead to further acceleration of the economy.

Now let us look at some examples of what the internet is bringing us presently. In the city of Nairobi, Kenya, *Huawei* is working with our local partners to build a much smarter and safer city, with a new mobile broadband network. Convergence command is dramatically improving the efficiency and reaction time of emergency services. Panoramic video surveillance and intelligent analytics is helping public security officers to conduct much more efficient and effective criminal investigations. Field officers are getting access to online files wherever they are carrying out their duty.

On another continent, Brazilian national power grid company, *Copel*, is building its network and data centers to convert itself to a smart-grid company fully connected with fiber-optics running at 400 gigabytes per second. The smart-grid offers on demand and real-time intelligent distribution power and quick fault diagnostics covering every corner of the grid no matter where the fault is. The annual power network downtime of cities and communities powered by *Copel* reduces from 2000 minutes to an unprecedented 3 minutes.

Yet another example, that the internet is changing, is the way that banks operate. Banks are often recognized as pioneers in terms of IT and networking applications, with data from decades of operation. The networked computing power big data analytics is providing the banks the means to quickly adapt to financial incidents and opportunities. The largest personal bank in China, *China Merchants Bank*, now can reduce credit check time form three weeks to ten minutes. *Industry and Commercial Bank of China*, the largest bank in the world, now executes online transaction of 380 trillion Chinese yuan every year. All these stories will soon become the past by 2025. With the 5G mobile network we will be able to connect 100 billion things in the world together, which is more than 14 times our current population. Everything electrically powered will have a chance to be connected by then. All wireless and wire-line connections will be running at unprecedented speed. This will result in another industrial revolution comparable to every industrial revolution in the past.

5G will bring ultra-high definition video to your mobile device. If you were to have a car accident you would not have to wait for representatives of the insurance company to come on-site. Simply use your mobile phone to feed the live video showing the scratch details to the service centers of the insurance company and you can finish the reporting in minutes. It will save time for you and save money for the insurance company. If you decide to sit down to watch a football game in your living room instead of your mobile device, the optical network will bring you the live game projected to the size of a wall in your living room. Human-sized players and figures will become the new standard for TV programs.

Wireless technology will also change the way we transport. With greater bandwidth and less latency of wireless signal connections, more locomotives can be used to drive much longer trains. Think of a 2.5 kilometer long train carrying 20,000 tons of goods. That’s more than three times greater efficiency in using the railways to drive your economy.

Having said all that, the world will not change automatically. Right now we still have 4.4 billion people unconnected, translating to 1.1 billion unconnected households. 90% of them are in developing countries, including China. To connect billion devices

in 2025 using 5G technology, there will be both engineering and policy challenges that we must overcome.

On the engineering side the hardship is visible. This is an award-winning picture from *Huawei*'s internal employee photography contest. A bunch of *Huawei* engineers were carrying an oil-electrical power generator to the top of a hill in order to restore power to our base stations. A blizzard blacked out the village and before the power could be restored, the communication had to be restored first to allow the villagers to ask for help. When the communication network is becoming so vital to support our society, our engineers' job is not simply about sitting in fancy laboratories and writing computer programs.

On the policy side, the job can be equally challenging. An open investment environment, friendly to foreign trade, is critical to bringing world-class internet technologies to a country. If industrial enterprises do not receive the internet infrastructure it requires to compete in the new world, the industrial revolution could turn into a lake of fire and they could end up as frag. But, with a well-built internet infrastructure, they will have equal footing to face challenges. If we embrace the technology, the technology will reward us.

On the other hand, like protecting other vital resources like air and water, regulations also need to be deliberately drawn to protect the network from being misused. Things can never be hacked only when they are not connected. Misusing the internet will only undermine the efforts of technology and slow down the revolution itself.

Finally, as a brief introduction of *Huawei*, we are dedicated to provide the best ICT solutions to serve our telecom enterprises and consumer customers. We will build networks in more than 170 countries and connect one-third of the global population. We are obsessed with innovation and bringing new technologies to the world every day. Thank you very much.

President: I thank Mr. Fan for his introductory statement. Now I invite our next panelist, Mr. Richard Desgange of ICRC to present his statement.

Mr. Richard Desgange, Regional Legal Advisor, ICRC, Beijing: Mr. President, Mr. Secretary-General, Mr. Deputy Secretary General, Your Excellencies, Distinguished Delegates, Ladies and Gentlemen; At the outset, we would like to take this opportunity to thank the Asian-African Legal Consultative Organization (AALCO) and the Government of the People's Republic of China for giving the International Committee of the Red Cross (ICRC) the opportunity to take part in AALCO's 54th Annual Session, in particular, this special meeting on International Humanitarian Law in Cyberspace.

I will address four points in the next few minutes: 1) what is cyber warfare? 2) what limits does International Humanitarian Law (IHL) impose on cyber warfare? 3) some of the challenges in applying IHL to cyber-operations; and, 4) some concluding remarks.

What is "cyber warfare?"

Businesses, media and governments regularly report that their websites or networks have been subject to cyber-attacks. However, there is no authoritative definition of the notions of "cyber-attack" or "cyber warfare" and they have been used by different people to mean different things. A large proportion of operations referred to as "cyber-attacks" constitute illicit information gathering-such as industrial espionage-or other cyber-crimes, and occur outside the context of armed conflicts. They are not governed by IHL.

In our context, "cyber-warfare" is used to refer to means and methods of warfare that consist of operations against or via a computer or a computer network through a data stream, when such cyber operations are conducted in the context of an armed conflict within the meaning of IHL. Put otherwise, cyber warfare is the use of computer codes to cause death, injury, destruction or damage during armed conflicts. It is only in the context of armed conflicts that IHL. Cyber warfare is thus only one aspect of the broader cyber security debate.

What limits does International Humanitarian Law impose on cyber warfare?

By prohibiting the threat or the use of force, the United Nations Charter imposes fundamental limits to States' resort to cyber warfare. These limits are part of what is usually referred to as *jus ad bellum*. As I am sure you all know, *jus in bello*-international humanitarian law-regulates the conduct of hostilities independently of questions of *jus ad bellum*. It put constraints on the belligerents' choice of means and methods of warfare with a view to protecting civilians as well as combatants.

Cyber-operations during armed conflict are subject to IHL in the same way that any new weapons, means and methods of warfare are. Article 36 of the First Additional Protocol provides notably that in the study and development of new weapons, means and methods of warfare-a State Party has to determine whether its employment would, in some or all circumstances, be prohibited by the Protocol or other rules of international law. Beyond the specific obligation is imposed in terms of legal review of means and methods of warfare, this rule shows that IHL applies to the use of technology in armed conflicts.

It should be stressed that asserting IHL applies to cyber warfare is not an encouragement to militarize cyberspace, nor does it legitimize cyber warfare; quite the contrary. By asserting that IHL applies, we reaffirm that limits exist if and when States would resort to cyber operations during armed conflicts. Such assertion constrains rather than legitimize cyber warfare. Indeed, the cardinal principle of conduct of hostilities under IHL is the obligation to direct attacks against combatants and military objectives only. Attacks against civilians and civilian objects are prohibited and this prohibition also governs cyber-attacks.

In recent years, there has been increasing concern for the protection of critical infrastructures against cyber-attacks. During armed conflict, such attacks would most often constitute violations of IHL. Indeed, drinking water and electricity networks that serve the civilian population, banks, railway networks and public health infrastructure are civilian objects in the first place (at least as long as they have not become so called "dual-use objects". As such, they are protected against direct attack. Water systems, in particular enjoy special protection for being objects indispensable to the

survival of the population. Similarly, dams and civilian nuclear plants do not usually fall within the definition of what constitutes a military objective, and are thus protected against direct attacks.

Without prejudicing on whether States will agree on specific norms regulating their behaviour in cyberspace to recall that IHL applies to a cyber-operation during armed conflicts reaffirms that existing international law already puts important limits to such operations.

However, to apply pre-existing legal rules to a new technology also raises the question of whether the rules are sufficiently clear in light of the technology's specific characteristics and foreseeable humanitarian impact. We cannot rule out that there might be a need to develop the law further to ensure that the protection it provides to the civilian population is sufficient. This will have to be determined by States.

Challenges for the interpretation and application of IHL

To re-affirm the relevance of IHL for cyber warfare and recall such fundamental rules is only the first step. Indeed, cyber warfare raises a number of challenges for the interpretation and application of IHL. Let me mention some of them.

Anonymity

Anonymity in cyberspace is easy to achieve, and this complicates the ability to attribute aggressive activities to the perpetrators and especially to do so in a timely manner. Since IHL relies on the attribution of responsibility to parties to an armed conflict, anonymity may create major challenges. If the perpetrator of a given cyber-operation cannot be identified, it may even be difficult to determine whether IHL is applicable to the operation. The answer to this challenge might, however, not lie in the legal field alone, but first in the technical field.

Do cyber operations amount to a resort to armed force triggering the applicability of IHL?

There is no doubt that armed conflict exists where cyber operations are resorted to in combination with traditional kinetic weapons. However, when the first-and possibly the only-hostile act is a cyber-operation, can this amount to an armed conflict in the meaning of IHL? This question is closely related but nevertheless distinct from whether a cyber-operation alone could amount to a "use of force" or an "armed attack" under the United Nations Charter. Such jus ad bellum issues are of crucial importance and thus widely debated. However, issues pertaining to jus ad bellum and the question of scope of application of IHL should not be confused.

IHL applies in situations of armed conflicts, whether international or non-international, as defined in international humanitarian law. In that regard, there seems to be no reason to treat cyber-operations that would cause effects similar to those caused by kinetic operations differently than the latter. Beyond such kind of operations, the disruption of critical infrastructure as a resort to armed force triggers the applicability of IHL-in view of IHL's purpose to protect the civilian population against such consequences. Defining the type of cyber operations that would trigger

the applicability of IHL in the absence of any kinetic operation will be determined through future State Practice.

Definition of a "cyber-attack"

In situations where IHL applies, such as when an armed conflict is already being waged through traditional kinetic means, the question that arises as to the definition of "cyber attack." The notion of "attack" is cardinal for the rules on the conduct of hostilities in particular for the application of the principles of distinction, proportionality and precautions in attack. Indeed, while parties to a conflict have to take constant care to spare civilians in all military operations and to protect them against the effect of hostilities apply to "attacks." In the 1977 First Additional Protocol defines attacks as "acts of violence against the adversary, whether in offence or in defence." (Art 49 (1)).

The group of experts which drafted the Tallinn Manual on the International Law Applicable to Cyber Warfare defined a "cyber attack" under IHL as a "cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to a persons or damage or destruction to objects." The crux of the matter, as often, lies in the details namely what is "damage " in the cyber world.

A number of IHL experts agree that the loss of functionality of an object may also contribute damage while others argue that only physical damage is relevant. The ICRC considers that if an object is disabled, it is immaterial whether this occurred through destruction or in any other way. This issue is very important in practice, as a more restrictive view of the notion of attacks might imply that fewer and less precise IHL rules would govern and thus restrict each type of operations. In particular, a cyber-operation aimed at making a civilian network dysfunctional might not be covered by the IHL prohibition of directing attacks against civilian persons and objects under an overly restrictive understanding of the notion of attack.

Interconnectedness

The interconnectedness of cyber-space creates specific challenges for the application of IHL rules. The same networks, routes and cables are shared by civilian and military users. It might even make it impossible to distinguish between military and civilian computer networks when launching a cyber-attack; if carried out nevertheless such an attack would violate the prohibition of indiscriminate attacks. The use of malware, which replicates itself without control and damages civilian cyber networks, is similarly forbidden. For example, a party to a conflict would violate the prohibition of indiscriminate attacks if it release via the internet a malware tailored to block enemy radars, while expecting that the malware's code will spread to and affect air civilian traffic control radars.

Furthermore, when launching an attack, parties to the conflict have to take all feasible precautions to avoid or at least minimize incidental civilian casualties and damage to civilian objects, including civilian cyber-infrastructure and networks. The interconnectedness of cyberspace that entails the risk that cyber-attacks causes incidental damage indirectly. Such indirect incidental damage, however remote it is, has to be considered to the extent that it can be expected and parties to the conflict

that plan or launch cyber-attacks have to expect that they risk causing incidental damage indirectly. One could even question whether it is always possible to appropriately assess such indirect effects.

This is just a brief overview of the issues and there are many other challenges, such as the geography of cyber conflicts, the application of the law of neutrality and the concept of sovereignty, or the definition and legal review of cyber weapons, just to name a few.

Despite these challenges, the key question is not whether new technologies are inherently good or bad. A holistic reflection is warranted to fully consider the risks and implications of the use of new technologies in armed conflicts from all perspectives and States should consider them well before they develop such technologies. While the relevance of IHL as the main body of law that constrains cyber warfare and protects civilians needs to be reaffirmed, there might be a need to develop the law further to ensure that the protection it provides to the civilian population is sufficient. That will have to be determined by States. In that regard, there is some debate within the international community on the manner to address the challenges raised by cyber warfare and more broadly those related to information security.

These challenges also underline the necessity for parties to armed conflicts to be extremely cautious, if and when resorting to cyber operations to avoid harm to civilians and civilian networks. They underscore the importance that States, which may develop or acquire cyber warfare capacities for offensive or defensive purposes, assess their lawfulness under IHL, as is necessary for any new weapons or methods of warfare. This is required by Art. 36 of the 1977 First Additional Protocol, and is the only way to ensure that armed forces and other governments agencies possibly resorting to cyber capabilities during an armed conflict will be able to abide by their obligations under international law. The fact that a growing number of States are developing cyber warfare capabilities only reinforces the urgency of these concerns. Thank you for your attention,

President: I thank Mr. Desgange, the Regional Legal Advisor for ICRC, for his presentation. Dear colleagues, we have now had two presentations; Mr. Fan presented us with the issues from a technological perspective, and Mr. Desgange has presented us the issue from a legal perspective. After listening to the two of them, I am now opening the floor to comments from the delegations of Member States. I notice that the first speaker is from China. You have the floor.

The Delegate from China: Thank you, Mr. President. Distinguished Delegates; Ladies and Gentlemen,

International law in cyberspace is at present a hot topic in international law and international relations. The Chinese Delegation has taken note of the first report on the agenda item of "international law in cyberspace" prepared by the Secretariat. We would like to thank the technical expert from Huawei Technologies Corporation of China and the legal expert from the ICRC for their presentations on the topic at this meeting.

The special meeting on "international law in cyberspace" highlights the importance of this issue and the urgent need to address it. At the initiative of the Chinese Government of the People's Republic of China, the item "international law in cyberspace" was firstly incorporated into the agenda of AALCO at the Tehran Session held last year. Preliminary exchanges of views on the item have also taken place between Member States. Although it has only been half a year since the Tehran Session, many important international conferences on cyberspace have been held, and various incidents emerged one after another. The international community is attaching increasing importance to the international rules on cyberspace. The first World Internet Conference successfully held in November 2014 by the Chinese Government in Wuzhen, established an international platform for the inter-connectivity of internet between China and the rest of the world, as well as a domestic platform in China for the sharing and governance of the international internet. In January 2015, China, Russia, Kazakhstan, Kyrgyzstan and Uzbekistan jointly submitted an updated draft version of the *International Code of Conduct for Information Security* to the UN General Assembly, which elaborates on the norms and principles governing the responsible behaviour of States in cyberspace. Currently, the UN Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (the UN GGE) is holding discussions over this draft report, and the "London Process" is holding its Global Conference on Cyberspace in the Hague. International law in the Cyberspace has been included as an important agenda item at both conferences.

This special meeting focuses on four key issues. Here I would like to elaborate on the position of the Chinese Delegation respectively as follows:

First, a UN-Centric governance model on cyberspace; Cyberspace is a *sui generis* domain, with the dual characteristics of reality and virtuality and also the dual nature of sovereign and common space. On the one hand, as an inter-connected and indivisible global information channel, cyberspace, which is shared by the global netizen, possesses the characteristics of global commons. As opposed to the outer space, the High Seas, the Antarctic and other global commons, cyberspace does not have any inherent territory. Cyberspace is an artificial and virtual space, which is formed by the intertwining of cyber activities of human beings on the basis of internet facilities. The orderly functioning of cyberspace concerns the interests of all States, which should not be appropriated by any single State. On the other hand, cyberspace has a sovereign nature. Each State is entitled to exercise sovereignty over cyber infrastructure, network data, cyber activities and internet governance within its territory. Each State may also exercise extra-territorial jurisdiction over cyber activities pursuant to international law. Therefore, the international cyberspace should be governed by sovereign States and the international community.

The Chinese Government is supportive of making full use of the existing mechanisms under the UN framework such as the ITU, the IGF and the WSIS process, taking into account the interests of multi-stakeholders, including those of different States, the private sector, the technological community and civil society, and coordinating responsibilities and functions of different platforms and mechanisms on internet governance, so as to build a harmonious order for cyberspace. We welcome the globalization efforts by the ICANN and the United States' announcement in 2014 of its intention to transfer the stewardship of the ICANN. We take these steps as initial

progress in the long-lasting joint efforts by the international community. The Chinese Government calls upon Asian-African States to participate in the process of global internet governance led by the United Nations and its specialised agencies in a more active manner, enhance our representation of an equal, just and reasonable international order of internet governance.

Second, State sovereignty and fundamental freedom of speech and expression in cyberspace; The principle of State sovereignty is the cornerstone of the contemporary international relations and international law, which, as a rule, is applicable to cyberspace. In this regard, the report put forward by the UN GGE in 2013 affirms that State sovereignty and derived international norms and principles can be applied to relevant activities conducted by States on the technology of information and communication, and is also applicable in the jurisdiction of countries over the infrastructure of technology of information and communication. The above-mentioned consensus marks that important progress has been made on the application of the principle of sovereignty in cyberspace.

State sovereignty is the combination of rights and obligations, which means that the application of State sovereignty in cyberspace implies both the enjoyment of rights and the assumptions of obligations. States are entitled to rights of sovereignty in cyberspace, including but not limited to the following: rights of sovereignty over cyber infrastructure; cyber data; cyber activities and internet governance; extra-territorial jurisdiction under international law over cyber activities outside one's territory; the right to self-defence; the right to invoke counter-measures; the right of State to equally participate in internet governance and international law-making.

State sovereignty in cyberspace also implies that States are to fulfil their obligations accordingly, which include but not limited to the following: first, respect for the sovereignty of other States, including that States shall not knowingly allow cyber infrastructure located in its territory to be used for acts that adversely and unlawfully affect other States; secondly, the obligation to ensure the peaceful use of cyberspace and to refrain from the threat or use of force; thirdly, the obligation of non-intervention by means of cyberspace; last but not the least, States should respect and protect human rights and freedoms, including the freedom of speech and expression.

The freedom of speech and expression is a fundamental right that has been enshrined in international human rights instruments. In accordance with relevant international law, it is forbidden for citizens, in exercising such right, to endanger national security, public order, as well as the lawful rights and freedom of others, including rights of privacy and intellectual property. The freedom of speech and restrictions thereupon are equally applied to cyberspace. Therefore, State sovereignty on cyberspace does not exempt States from their obligations. Also, there is no absolute freedom of speech and expression in cyberspace. The Chinese Government supports the freedom of speech and expression in cyberspace, and at the same time, maintain its position on striking a balance between national security, public order in cyberspace and the freedom of speech and expression of individuals.

Third, the application of the existing rules of armed conflict; There is no legal vacuum in cyberspace. Existing international law, including the Charter of United Nations, applies in principle to cyberspace. This has already been explicitly presented in the

statements put forward by UN GGE in 2013. In recent years, the issue of cyber attack has attracted increasing attention of the international community. Some States and scholars, however, have exaggerated the issue, by categorically describing cyber attacks as cyber warfare, invoking the provisions of the Charter of the United Nations on the threat of use of force or armed attack, and advocating the application of *jus ad bellum*, *jus in bello*, and in the law of State responsibility to cyber attacks. This "military paradigm" in response to cyber attacks has aggravated arms race and the militarization of cyberspace.

"Cyber warfare" is the severest form of confrontation between States in the cyberspace. That said, it is not that case that all cyber attacks are acts of States constituting "cyber warfare". In fact, most cyber attacks are committed by individuals or other non-State actors. Such cyber attacks that are generally regarded as cyber crime or infringement of cyber rights should be regulated by domestic criminal laws or the law of torts. Even of some of these attacks are committed by States or may be attributed to States, most of such attacks fall below the threshold of "threat of use of force" and "armed attack"; rather, they only are cyber attacks of minimal level of intensity, which may only constitute other internationally wrongful act such as espionage. These attacks should be first addressed by taking non-military measures such as counter-measures and sanctions, rather than resorting to force. In certain situations, even if the cyber attacks are suspected of constituting a "threat of use of force" or "armed attack", due to the anonymity and the difficulties in attribution, substantial uncertainties exist as to the source and identification of attackers. To date, State practice concerning cyber warfare is still scarce, and whether relevant rules can be applied to the so-called "cyber warfare" would require further exploration with great caution.

Regarding the use of force in cyberspace, *lex lata*, including *jus ad bellum* and *jus in bello*, applies in principle to cyberspace. At the same time, there is a need to adopt new rules on cyber-Wild West. China hopes that we, nations in Asia and Africa, could actively participate in international law making on cyberspace. As a matter of priority, our current task is to clarify which existing rules of international law are applicable to cyberspace, and seek consensus among Asian and African States on the areas or issues of priority to be addressed.

Fourth, international cooperation in combating cyber crimes; the international community should make joint efforts to deal with the common challenge posed by cyber crime. The Chinese side notes the Budapest Convention on Cyber Crime that has been referred to in the document of the Secretariat. China acknowledges that, the Convention, as the only existing comprehensive multilateral treaty that specifically deals with cyber crime, plays an important role in promoting regional cooperation in fighting against cyber crime. However, it is undeniable that the Convention has its drawbacks. First of all, since the Convention was formulated mainly by western developed countries without the participation of the developing countries, our concerns and requests have not been taken into consideration. Secondly, provisions in the Convention that States may conduct cross-border investigation without the consent of the territorial State would jeopardize the judicial sovereignty of a State. Therefore, the Chinese side supports negotiating an international convention on combating cyber crime under the framework of the United Nations with the above-

mentioned Budapest Convention serving as a reference for the drafting of the new convention.

In conclusion, the clarification of *lex lata* and *lex ferenda* is the common challenge encountered by all nations. As the important stakeholders in cyberspace, Asian and African States should actively participate in related discussions and strive for the voice and influence that match their status. The Chinese Government, therefore, proposes establishment of a working group on international law in cyberspace within the AALCO, with a 2-year mandate to study and explore issues such as the application of existing international law in cyberspace and the development of international law in cyberspace. This working group is intended to build consensus between Asian-African States to formulate principles and suggestions that meet the common interest of all parties, and to produce an outcome document to the 2017 Annual Session. The Chinese Government looks forward to conducting extensive exchange with all parties on this issue, and would like to work together with all parties in order to seek broader consensus on the resolution of this Annual Session. Thank you, Mr. President.

President: I thank the distinguished representative of China for his statement. I now give the floor to the distinguished representative of Japan. You have the floor Ambassador.

The Delegate from Japan: Thank you, Mr. President. Distinguished Delegates, Ladies and Gentlemen; My delegation is pleased to participate again in the deliberation of this important agenda item. We greatly appreciate the informative presentations by the two distinguished panellists this morning.

As we stated in our previous intervention on this subject at last year's Annual Session, we consider that cyberspace serves as a basis for socio-economic activities. Securing free flow of information in cyberspace is one of Japan's basic policies. The international community has been striving to build a safe and reliable cyberspace by securing its openness and interoperability without States' excessive control or restriction, while giving due attention to strike a balance between the protection of privacy and assurance of security.

Japan is aware of the risk, such as the cyber attack against Sony Pictures Entertainment, against the stable use of cyberspace as one of the urgent security issues that no single country can address by itself. Under these circumstances, Japan has been actively engaged in the discussion on the scope of application of existing international law to cyberspace in the UN Cyber Group of Governmental Experts (CGGE) and has also recognized the need for further dissemination of the Budapest Convention on Cybercrime in order to address cybercrime in concert with the international community.

We believe that Cyberspace has been a driver for social and economic growth as well as innovation, which has been led by the private sector. In order that cyberspace continue to be the driver for social and economic growth, it is essential to maintain an open and transparent environment based not on multilateral, but multi-stakeholder approaches that all stakeholders, such as civil society, academic, private company, NGO and government should participate in the process.

I wish to give our view on a few important specific issues.

First, with regard to sovereignty and freedom of cyberspace: a State where cyber infrastructure or person using cyberspace are located can exercise territorial sovereignty over such infrastructures or persons. Freedom of expression and secrecy of correspondence (confidentiality of communication) should be respected to the maximum extent possible as fundamental human rights. However, these fundamental human rights are not guaranteed without limitations. If there are higher legal interests, they can be limited for the purpose of public welfare.

Second, with regard to peaceful use and militarization of cyberspace: addressing various threats in cyberspace is an urgent issue in the international community. Application of existing international law should be further considered for the stable use of cyberspace. Moreover, States are encouraged to take confidence-building measures (CBM) bilaterally and multilaterally to prevent unintended escalations that are not intended by parties.

Third, cybercrime and Budapest Convention: cybercrime is a transnational threat that needs to be tackled jointly by the international community. The convention on cybercrime of the Council of Europe, or the so-called Budapest Convention, to which the AALCO Secretariat briefing paper also refers, is so far that only effective multilateral instrument on the use of cyberspace. We believe that, if more countries harmonize their domestic legislations to the standard of the Budapest Convention, it will contribute greatly to the stable use of cyberspace.

Japan participated in the negotiations process of the Budapest Convention and finally acceded to the convention in July 2012. We are currently the only Party from the Asian region to this convention but gradually more and more non-European countries are adopting the standards of Budapest Convention in their domestic legislations. Other non European Parties to the convention so far include the United States, Australia, the Dominican Republic, Panama and Mauritius. South Africa and Canada also signed the Convention.

We believe that the Convention is based on universal needs of the practitioners working on cybercrime investigation and prosecution and that can be applied in any countries around the world, including both developed or developing countries, as the universal standard for cybercrime investigation and prosecution.

With respect to the proposal to develop cybercrime convention at the UN level, our belief is that if we consider the urgent need of assistance for many countries in terms of cybercrime legislations and capacity building of law enforcement agencies, we should be prudent so as not to duplicate the efforts to create something very similar to the Budapest convention. Thank you very much.

President: I thank the distinguished representative of Japan for his statement. Now I give the floor to the distinguished representative of the Republic of Korea.

The Delegate from the Republic of Korea: Thank you, Mr. President. My delegation appreciates the quality of the initial analysis of this complex issue-area

conducted by the Secretariat in a brief period of time. I'd like to thank the two panelists for the precious presentation.

Because of the transboundary effect of cyber operations, most of the problems arising in cyberspace have international or global dimensions, threatening sovereignty and security of States, as well as privacy, human rights and economic interests of individuals. In particular, because of the digital-divide, which is ever widening, developing countries are especially vulnerable to the damages caused in cyberspace. However, development of international legal regimes regulating cyber operations has fallen far behind the development of abuses of ICT. My delegation is conscious of the urgent necessity of establishing international governance of cyberspace.

In abstract, the concept of sovereignty, the principles and rules of State responsibility, the Charter of United Nations, the rules of international humanitarian law etc., can largely be applied to human activities in cyberspace, as suggested by a group of experts in Tallin Manual.

However, conceptual applicability is not enough to regulate effectively human activities in cyberspace. Because of the particular characteristics of cyber operations, it is extremely difficult to make operational rules regulating activities of State or non-State actors in cyberspace. Even though a certain rule of international law is conceptually applicable to a certain category of cyber operations, it is not easy to establish causal relationships between a particular cyber operation and its consequences. In such a case the rule is neither operational nor enforceable. Even in domestic legal system, it is difficult to make sufficient legal rules regulating human activities in cyberspace.

Considering the difficulty of designing governance of cyberspace due to these characteristics of activities in cyberspace, my delegation is of the view that it is desirable for us, the delegations to the AALCO meetings, to be very realistic and cautious in developing ideas for international governance of cyberspace.

It would be better to begin by reflecting on the general approach to the issue-area, and, we might begin by examining the possibility of applying the existing rules of international law to the activities of State or non-State actors in cyberspace, and the limits of such application.

Considering unlimited variety of human activities in cyberspace, it would be preferable for us to confine the scope of our deliberations to a certain extent in the initial stage. In this regard, my delegation considers the draft resolution this agenda item, prepared by the Secretariat, indicates a good orientation for deliberations, which will be a long and difficult journey. Thank you.

President: I thank the distinguished representative of the Republic of Korea for his statement. Now, I give the floor to the distinguished representative of Kenya. You have the floor.

The Delegate from Kenya: Thank you, Mr. President. Allow me to join the other speakers in congratulating the AALCO Secretariat in presenting this important topic on "International Law in Cyberspace". Similarly, Mr. President, allow the Kenyan

Delegation to thank the Secretariat for the publication for the special issue in the AALCO Journal of International Law on the topic "Cyberwarfare and International Humanitarian Law". The topics covered in that book are very useful to the discussions we are having today.

Mr. President, Kenya welcomes the special half-day forum to discuss international law in cyberspace and, in particular, Kenya supports the need to have a multilateral treaty that effectively prevents escalation of cybercrime, preferably through a UN-centric governance model for cyberspace. Kenya recognizes that cyberspace plays a critical role in the global economy. It has national and international dimensions that include industry, commerce, intellectual property, security, technology, culture, policy, and diplomacy. As such, Mr. President, it has its own distinct characteristics and challenges that emerge even as technology advances on a daily basis.

Distinguished delegates, Kenya recognizes the importance of these developments in international law and, as a nation, we are actively encouraging its continued growth through national initiatives, such as the Kenya Vision 2030, Information-Communication Technology Masterplan, and the recent deployment of a nation-wide fiber-optic network infrastructure. Kenya's Informational-Communication Act has been established to facilitate the development of the information and communication sector and the need to protect the privacy of information.

Distinguished delegates, as Kenya moves further into becoming an information, communication, and technology-oriented society, cyber-threats have become glaring. Without a proper legal regulatory framework, cyber-criminals the world over are bound to exploit countries' ICT vulnerabilities. While these actors seek to illicitly access, alter, disrupt, or destroy sensitive personal, business, or government information, the country is working diligently to effectively enhance the means of protecting information in order to counter today's cyber-threats, from within and out of the country.

Distinguished delegates, in response to these threats, and in direct support of the national priorities and ICT goals, Kenya has developed a national cyber-security strategy. The strategy defines the nation's key objectives: an ongoing commitment to support national priorities through ICT growth, while at the same time aggressively protecting critical information infrastructure. The Government of Kenya is committed to the safety, security, and prosperity of our nation and its partners. Kenya views cyber-security as a key component for upholding that commitment, thereby providing organizations and individuals with increased confidence in online and mobile phone transactions, encouraging foreign investment, and opening a broader set of trade opportunities within the global marketplace. Successful implementation of the national cyber-security strategy will further enable Kenya to achieve its economic and societal goals through a secure online environment for citizens, industry, and foreign partners, to conduct business.

Distinguished delegates, Kenya has for a long time relied on physical evidence to arrest cyber-criminals; a move that has stifled efforts towards reduction of the vice. Cyber-criminals require expert cyber-surveillance since it is hard to physically detect both international and local cyber-criminals. Kenya is therefore in the process of bringing into law the "Cybercrime and Computer-related Offences" bill. This law

seeks to address offences against confidentiality, integrity, and availability of computer data and systems. It also seeks to curb cyber-stalking, hate-speech, and identity-related crimes. The bill will be the most effective cyber-security law in Kenya, as it aims to concentrate on ways of getting electronic evidence against the accused.

Distinguished delegates, as a region, East Africa has recognized the emerging challenges of cyber-criminal activity, and each of the East African States is at various stages in the development of their cybercrime legislation. The East African States also held a regional workshop recently to discuss cyberspace security, and the States resolved to increase collaboration with the view of promoting intervention to meet the needs of all African legislative jurisdictions in the matter of cybercrime legislation. The States also recognized the need to ratify the Budapest Convention on Cybercrime, and to domesticate its provisions. Finally, the States undertook to encourage their respective law-enforcement agencies to enhance transborder operations with a view to promoting faster responses to cybercrimes through the sharing of information, experiences, and good practices.

In conclusion, the African Union has developed the Convention on Syber-security and Personal Data Protection, which addresses cyberspace-related matters, including data-protection and the prevention of cybercrimes in line with the increasing adoption of similar legislation in other parts of the world. The Convention also recognizes the need for the African Union to create a legislative framework that will enable Member States to participate in the digital economy, while at the same time protecting the fundamental rights of individuals in relation to their personal data. The AU Convention creates a framework that enables Member States to combat cyber-risks and cybercrime. Kenya supports this Convention, which we believe will address the transboundary cyberspace crimes. Thank you, Mr. President.

President: I thank the distinguished delegate from Kenya. I now give the floor to the distinguished delegate from Iran.

The Delegate from The Islamic Republic of Iran: Thank you, Mr. President. In the name of God, the most compassionate, the most merciful; Your Excellency, Prof. Dr. Rahmat Mohamad, the Secretary General; Mr. President; Distinguished Panelists;

I would first like to express my appreciation for the enlightening and informative report and presentations given by the distinguished panellists. My delegation would like to thank the Secretariat for the serious consideration of the new item "International Law in Cyberspace" and the comprehensive report on the topic. The Islamic Republic of Iran attaches high importance to the issue and believes that its serious and effective consideration by AALCO can help shape the rules of international law applicable to cyberspace.

Mr. President, the exponential expansion of technology in recent years has created an increasingly interconnected world. While efforts to regulate cyberspace at the international level have spanned miscellaneous spheres of international law, the Islamic Republic of Iran believes that AALCO Member States could expand the debate on the issue to cover such diverse questions as possible applicability of existing rules of international law to curb cyber-attacks, the strengths and weaknesses

of international humanitarian law *vis-à-vis* cyber warfare and the regulation of cybercrimes.

Mr. President, enjoying all features of *res communis omnium*, cyberspace is without borders. State jurisdiction in such a virtual universe is therefore exercised by every single State based on other links, i.e. their physical territories, their nationals, and the control they exercise upon individuals' activities. The elusive feature of this type of jurisdiction requires that it be controlled by all States. The dominance, or ownership, of a single State with respect to the Internet may undermine the sanctity of sovereignty and calls into question whether a new scheme should replace the current one. That is why the Islamic Republic of Iran believes in the multilateral management of the Internet. We believe that the very existence of cybernetic services must be rooted in, and accompanied by, respect for territorial sovereignty of States, described by the International Court of Justice in its decision in *Corfu Channel case* to be 'the foundation of international relations', and emphasized as such on the 2013 report of the UN Group of Governmental Experts on Information Security. Therefore, serious efforts are needed to amend the current system provided by Internet Corporation for Assigned Names and Numbers (ICANN) and these must be founded on conviction. We believe that the first step in curbing cyber-attacks is the exercise of sovereignty by every single State, within its borders, without supremacy given to a single State by way of unlimited powers over cyber activities of other States.

That said, while cyber security requires every State to protect itself against cyber threats, email correspondence and all kinds of data stored in the virtual space must remain protected and free from supervision by the providing entity. Article 24 of the Vienna Convention on Diplomatic Relations on the inviolability of archives and documents is also consistent with such interpretation. In this regard, views of some States at the debates on the topic "Consideration of effective measures to enhance the protection, security and safety of diplomatic and consular missions and representatives" at the Sixth Committee of the UN General Assembly in October 2014 have been expressed to that effect.

Mr. President, while cyber-attacks may be directed by State or non-State actors against the infrastructures of other States in time of peace or in wartime, the question remains on the applicability of rules of international humanitarian law to instances of so-called cyber warfare. Due to the heavy involvement of the so-called cyber warfare in the Internet of private sector and non-governmental organizations, an attack on any node of the system can be tantamount to the destruction of the entire infrastructure of a country including dams, electrical grids, nuclear power plants, air traffic control, communications, and financial institutions. It is therefore inevitable to State that rules of international humanitarian law, i.e. rules derived from the Hague Regulations of 1907, or Geneva Conventions of 1949, do apply to cyber-attacks launched during military operations. However, due to the ubiquitous nature of cyber-attacks as a means and method of warfare, the launching entity is bound to fail to discriminate between civilians and military personnel or between civilian and military objectives. In such circumstances, as avoiding superfluous injury or unnecessary suffering or causing severe or long term damage to the environment is unmanageable, the question of compliance is far from certain. All that said, the threshold of armed conflict in cases of cyber-attacks in conventional peacetime is yet a more rudimentary question fraught with uncertainties.

For all these reasons, the Islamic Republic of Iran is of the view that despite the impossibility of creating a new treaty system from whole cloth to regulate cyber-warfare, dealing with details would require, without doubt, hard work on the part of all States and specifically AALCO Member States.

Mr. President, equipped with a comprehensive law on cybercrimes adopted in 2009, the Islamic Republic of Iran has followed with interest the work of the UN Group of Governmental Experts on Cybercrimes, mandated by the UN General Assembly Resolution 65/230. My delegation hopes that the outcome of the working group deliberations, which includes a comprehensive study on the different aspects of the issue and possible solutions, would lead to a suitable global legal framework under the aegis of the UN to promote international cooperation. In any case, we maintain that consistent application of international rules is vital and oppose double-standards and selective application of international law in any form. Thank you, Mr. President.

President: I thank the distinguished delegate of Iran for his statement. Now I give the floor to the distinguished delegate of Malaysia.

The Delegate from Malaysia: Thank you, Mr. President. Malaysia welcomes the deliberation of this important topic after it was first introduced during the Fifty-Third Session of AALCO in Tehran in 2014. Malaysia will focus its intervention based on the AALCO Secretariat's Report AALCO/54/BEIJING/2015/SD/S 17 on three issues, namely: 1) the necessity and stability of a UN-centric governance model treaty; 2) importance of balancing sovereign rights of States and fundamental rights of freedom of speech and expression; and, 3) transnational cybercrime and the need for a multilateral treaty to effectively prevent its escalation.

Malaysia notes that both global and regional climate on cybercrime strongly suggests that there are strong initiatives for international instruments to be forged among Member States to ensure that countries are serious and well equipped to combat cybercrime. Developed Member States are not only looking at enacting adequate laws but also exploring on the possibility of harmonizing of laws to not only enable international cooperation to be rendered, but for it to be rendered expeditiously.

Malaysia is currently considering the implications of accession to the Budapest Convention, which came into force on 1st July 2004. Amendments are required to the relevant domestic laws in order to strengthen the regulation and governance of computer/ cyber crime for the purpose of considering accession to the convention.
Malaysia emphasizes a thorough review of substantial and procedural law at the national level to enhance its current capacity to address cybercrimes even if accession to the Budapest Convention is not a positive outcome.

Mr. President, Malaysia recognizes the importance of balancing sovereign rights of the States and fundamental freedoms of speech and expression of its citizens in cyberspace. Malaysia notes the view that the exercise of sovereignty by any States towards the cyberspace should take into consideration its citizens freedom of speech and expression.

Nonetheless, Malaysia would like to reiterate its views that such exercise of freedom of speech and expression, whether in cyberspace or otherwise, must be within reasonable restriction to address any threat to the peace and security of the country. As cyberspace had been used as a medium by the terrorist groups to preach, propagate, incite, promote, publicized and disseminate their extremist ideologies to the society, the issue of fundamental human rights and sovereign rights must be carefully balanced.

Mr. President, Malaysia notes that there may be other international initiatives to address cybercrime such as the proposed "UN Centric Governance Model for Cyberspace" and the need for multilateral treaty initiatives so as not to result in duplication of efforts similar to the Budapest Convention. Proper study should be given and a lot of commitment would be required from Member States to ensure its proper execution.

Nothing that cybercrime is transnational and transboundary in nature, Malaysia realizes the importance of having a formal legal framework on international cooperation. Hence at the national level, Malaysia has in place laws to cater for international cooperation such as the Mutual Assistance in Criminal Matters Act 2002 [Act 479] ("EA"). Malaysia has also put in place the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 [Act 621] to complement both the MACMA and the EA to facilitate the conduct of complex computer crime investigations and the ability to collect necessary evidence and cooperation for the purposes of confiscation of proceeds and instrumentalities of these crimes. These existing domestic legislations, which allow for international cooperation, are invaluable to facilitate the conduct of complex computer crime investigations.

Finally, Mr. President, Malaysia takes the view that unless countries in both our regions work together to render international cooperation, either under a multilateral, bilateral, or domestic legal framework, cybercrimes cannot be addressed effectively in our region and beyond. Thank you, Mr. President.

President: I thank the distinguished delegate of Malaysia for her statement. I now give the floor to the distinguished delegate of India.

The Delegate from India: Thank you, Mr. President. Excellencies, Ladies and Gentlemen; I thank all the panelists for their presentation and congratulate the AALCO Secretariat for the preparation of detailed background document on the topic and also the introductory statement made by the Deputy Secretary-General. Today's Special Meeting has identified three broad sub-topics, namely State sovereignty; peace of cyberspace and cyber crime to deliberate upon. The following are some of our thoughts on the topic based on the position we undertook in various fora.

Mr. President, the rapid growth of information and communication technologies (ICTs) has contributed immensely to human welfare, but has also created risks in cyberspace, which can destabilize international and national security. Global and national critical infrastructure is extremely vulnerable to threats emanating in cyberspace. Additionally, the growth of social media (Twitter, Facebook, etc.) has created a new medium for strategic communication that bypasses national boundaries

and national authorities. The global data transmission infrastructure also depends critically on the network of undersea cables, which is highly vulnerable to accidents and motivated disruptions.

In the late 2000s, the international community realized the importance of developing international norms to ensure that States behave responsibly in cyberspace, especially when cyber attacks had brought some of the countries almost to a standstill in many of their official functions. We firmly believe that cyberspace activities need to be addressed from both an international and a national perspective as it requires the concerted cooperation of the international community.

From an international law point of view, the relevance of the Charter of the United Nations and its applicability to various aspects of international cyber security has to be given adequate emphasis. The UN Charter, particularly Article 2(4) read with Article 51, provides a basic framework to maintain international peace and stability in order to promote an open, secure, and peaceful environment for cyberspace activities. A study of this framework may be useful in providing guidance to determine the norms pertaining to State behavior in the activities relating to international cyber security.

However, on the question of prohibition of 'use of force' under Article 2(4) of the UN Charter, there is no consensus as to the precise threshold at which cyber operations activities would amount to an internationally wrongful threat or use of force. Similarly, the interpretation of Article 51 with a view to accommodate cyberspace activities is fraught with many difficulties and fewer convergences. It is difficult to determine when a 'cyber attack' could be considered as an armed attack for the purpose of 'self-defense' under Article 51 of the UN Charter.

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 its territory. In this regard, categorization of cyber incidents and identifying the legal gaps are most important to address.

The concept of warfare is no longer restricted to armed attack in the traditional sense of the term. The crippling of critical information systems of a country, or cyber attacks that block government websites for a few hours, are also now being considered as methods of gaining military advantage. This only emphasizes the pressing need for internationally agreed rules to check cyber crime, cyber terrorism, and cyber warfare. There would, however, also be a corresponding need to also further work on the definitions of key terms in international law such as sovereignty, right to self-defense, use of force, armed attack, and combatants, so as to apply them in the cyber context.

While IHL rules seem to be the most suitable existing international regime that might be extended to cyber terrorism and cyber crime, it also has a large number of limitations and would most likely not serve as an effective means of addressing the pressing issue of cyber crime. Aside from these specific issues in extending IHL rules to the cyber context, IHL would also suffer from the general concerns that arise in application of international law.

The Budapest Convention (2001) is the only existing multilateral convention on cyber crimes. However, it has been criticized as being fundamentally unbalanced and its long-effectiveness has been brought into question on numerous occasions. For various reasons, India is not a Party to the Budapest Convention.

Mr. President, it is our firm belief that the core values of liberty, freedom of expression, and rule of law, apply equally to cyberspace and it is in our common interest to maintain a peaceful, secure, and resilient cyber space. To ensure this, we have put in place a robust institutional and legislative framework to facilitate e-commerce and also to deal with cybercrime and challenges to cyber security. The Government is also actively partnering with the private sector, industry associations, services providers and other stakeholders, to jointly try to secure cyberspace. At the national level, India has enacted a national legislation, the Information Technology Act, 2000 as amended in 2008 to deal with vital issues such as electronic transactions, digital signatures, cyber crimes, cyber measures for handling cyber-security and data protection. The Act also seeks to foster security practices within India that would serve the national interests in a global context.

India's computer emergency team's response team, called CERT-IN, operates on a 24/7 basis to undertake emergency measurer's security incidents in the country. Similarly, the National Association of Software and Service Companies (NASSCOM) and its member organizations have launched several initiatives, through the Data Security of India, to promote data protection and develop security and privatization to respond to privacy codes and standards. Taking cognizance of the significant growth in cyber breach instances in India, the Government came out with the National Cyber Security Policy (NCSP) in July 2013, which aims to facilitate a secure computing environment and guide actions for protection of cyberspace.

Mr. President, in order to move forward, we support the Secretariat's Resolution to establish an open-ended working group on the subject matter and further discuss it in the meetings or workshops. However, a clear mandate is required on the basis of which the working group can work and discuss specific issues which can then be considered at the next Annual Session of the Organization for this purpose. We propose to suitably modify Operative Paragraph 1 and incorporate it in Operative Paragraph 3 so that the open-ended working group and the relevant workshop can focus their efforts in the identification of relevant provisions of the UN Charter and other relevant instruments related to State conduct in cyberspace. And, analysis of such instruments should also be carried out and put up for consideration of the Fifty-Fifth Session of AALCO. I thank you, Mr. President.

President: I thank the distinguished delegate of India. I now give the floor to the distinguished delegate of Nepal. You have the floor.

The Delegate from Nepal: Thank you, Mr. President. Mr. President, Deputy Secretary General, and panelists; The delegation of Nepal wishes to appreciate the excellent documentation on rules of international law on cyberspace, as prepared by the AALCO Secretariat, and notes with appreciation the updates of the Deputy Secretary General. I would also like to appreciate and acknowledge the contributions of the panelists.

Mr. President, cyberspace has become an integral part of communication and interaction between peoples of the globe, with profound impacts on the national life of States in the present time. This has necessitated the development of a regime of governance of the internet with a view of equity, given that a digital divide exists in developing countries. From juridical perspective, States do have sovereign rights in cyberspace and their citizens do have freedom of speech and expression in cyberspace. All States, be they developed or developing, are facing a challenge, in one way or another, to strike a balance between them. On the other hand, in the recent times, cyberspace has been used for military purposes. A number of reported instances of resort to cyber-attacks by State and non-State parties to armed conflicts demonstrate, *inter alia*, that cybercrimes are being increasingly perpetrated.

Mr. President, the world has witnessed armed conflicts in land, in sea, in air and in airspace, and now in cyberspace. Some commentators have started terming this as the fifth domain of warfare.

Cybercrime may pose a number of threat to international information security. Such threats include development and use of information weapons, information terrorism, information crime, dissemination of information harmful to social, political, economic, spiritual, cultural, and moral systems.

From the standpoint of international law, States are now facing a range of challenges in relation to acts of cybercrime. What is the basis of jurisdiction over an act of cybercrime? How to conduct inter-State relations *vis-à-vis* this? Is Article 51 of the UN Charter applicable in case of cyber-attacks? How to balance security and human rights? And, of course, how, and to what extent, does IHL apply to cyberwarfare, and can cyber-attacks alone constitute armed conflicts? These are the questions before us.

The delegation of Nepal holds the view that the AALCO should be of assistance to Member States to address these issues in a uniform fashion. We believe that a mechanism such as an open-ended working group on international law in cyberspace should be formed so that deliberations on this issue are carried out effectively, leading to robust governance on the internet.

Finally, the delegation of Nepal wishes to place on record that AALCO should be a leading institution in the development and furtherance of appropriate and effective rules of international law to combat cybercrimes and of an international regime that assists the international community to have a robust mechanism and modality so that a proper balance between the State domain and public domain *vis-à-vis* cyberspace can be developed and maintained.

President: I thank the distinguished delegate of Nepal for his statement. I now give the floor to the distinguished delegate of South Africa.

The Delegate from South Africa: Thank you, Mr**.** President. We are pleased to discuss the topic of "international law in cyberspace", which was proposed by the People's Republic of China, and welcome that the emphasis will be on the developing elements in this topic. We would like to thank the Deputy Secretary General for his opening remarks, and the two panelists for making comprehensive and informative presentations on this topic.

Mr. President, noting the cyber-security challenges faced by the global community and individual countries alike, South Africa developed and approved the National Cyber-security Policy Framework in 2012. The Framework outlines the policy positions that are intended to: address national security threats in cyberspace; combat cyber-warfare and cybercrimes; develop, review, and update existing substantive and procedural laws to ensure alignment; and, build confidence and trust in the secure use of information and communication technologies. South Africa supports all initiatives to develop universal instruments under the auspices of the UN to address threats posed by cybercrime.

Mr. President, under the sub-topics, namely State sovereignty and cybercrime, South Africa wishes to make the following remarks:

Firstly, regarding State Sovereignty: while examining the possibilities of sovereignty in cyberspace, States have to bear in mind that cyberspace is neither immune from State sovereignty, nor can it be considered a global commons. The development of sovereignty in the sea, air, and outer space domains offers insights into how States sovereignty might develop in cyberspace. It is clear that an international regime is needed to successfully extend State sovereignty beyond a State's territorial area to these other domains.

Secondly, it is clear that combating cybercrime effectively will require global cooperation involving a broad group of countries. Existing international instruments contain elements that can be considered by each State when dealing with its legislative requirements to ensure a safe cyberspace for itself. While regional instruments are effective to address cybercrimes on an international basis, we can learn from this. Existing instruments for traditional crime can also not be extended to combat cybercrime; the reason being that various cyber-specific interventions are not covered in these instruments.

In conclusion, a comprehensive multilateral approach would be best to address the issue of cybercrime. Thank you, Mr. President.

President: I thank the distinguished delegate of South Africa for his statement. Now I give the floor to the distinguished delegate of Qatar.

The Delegate from Qatar:[2] Thank you, Mr. President. In the name of God, the most compassionate, the most merciful; Cyberspace represents a new strategic environment for the growth and the emergence of new forms of conflict. We can say that the international system is a phenomenon with multiple dimensions and scope of impact and this system now has greater complexity due to the phenomenon of cyber terrorism. This has raised questions regarding the extent to which the legal framework governing the 'use of force' can be applied to cyberspace. The Charter of the United Nations in Article 2(4) requires all Member-States to "refrain in their international relations, from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of

[2] This statement was delivered in Arabic. This is an unofficial translation made by the Secretariat.

the United Nations." Article 51 of the UN Charter also lays down conditions for the use of force.

Cyberspace is important in the global infrastructure of information, and is an important factor in the work of vital facilities of government. Additionally, the new digital economy is important to the progress of of global economic growth. At the came time, cyberspace has also become a means to launch an attack and implement hostilities between adversaries. In this way it has become like other areas such as space, air and sea – a new medium of conflict.

This has also led to the emergence of the new phenomenon of synchronization of global crime and terrorism, blurring the relationship between crime, which is traditionally understood to be solely for material profit, and terrorism, which is understood to be for political goals. Technological developments have led to the overlap between terrorism and crime. Communication and information technology networks have played a role in turning terrorism into a global threat. Terrorists have also used computers as tools to commit acts of cyber terrorism; tools such as computer viruses or spyware are used to hack sites, for information theft, money laundering, and other crimes.

The question thus posed is how international legal norms, which emanate from the Charter of the United Nations, can be applied to cyberspace, because the current legal framework is not enough to provide solutions to the security dilemma posed by the cyberspace security attacks.

Qatari measures to protect the cyberspace

The State of Qatar occupies an advanced position among countries in terms of the widespread use of Facebook and social media, in addition to the growth of e-commerce transactions at all levels. This trade is carried out using electronic documents, electronic signatures, electronic contracts, and in electronic virtual places on the information network, which has raised problems for the judicial system in how to deal with this huge amount of information.

For these reasons, the legislature needs to move quickly to develop legislation regulating all aspects of electronic transactions, and provide protection against criminal activities, which creates confidence and gives people a sense of peace and security with respect to their own lives as well as with their money and their interests.

The State also established provisions that will respond to local and international emergencies in order to protect cyberspace, and other devices to combat all forms of electronic crimes by tracking the perpetrators and dealing with the evidence arising there from.

1. Legislative measures

Qatar has passed many national legislations that are consistent with international instruments to which the State has acceded. Those legislations include a special law to counter cyber crimes – Law No. (14) in 2014. This new legislation criminalizes many things related to electronic crimes. It has categorized the crimes, defined sanctions,

punished interference and incitement, defined the moral obligations of persons, service providers, and institutions of the State, and set out the necessary punishments for non-compliance with the provisions of this law.

Qatar did not rush into the enactment of integrated legislations, but gradually developed it through several stages; the preliminary phase came through general provisions contained in the Qatari Penal Code No. (14) in 1971; then came the transitional phase for the protection of cyberspace through singling out a whole chapter of computer crimes in the Qatari Penal Code No. (11) in 2004; then came the phase of issuance of full cyber legislation under the name of "cyber crimes."

2. Cyber Security

One of the most important priorities of the State of Qatar is to protect the systems and infrastructure of information technology and communication, and for that the State established "Qatar's National Computer Emergency Response Team", known as "Q-CERT" in 2005. Qatar carries the torch to light up the way for other neighboring countries to establish similar centers in those countries.

The goal of Q-CERT is similar to, largely, civil defense forces. The State of Qatar establishes civil defense forces to respond to the occurrence of, for instance, a fire emergency, and it does not wait for the occurrence of damages to think about the appropriate way to respond. Q-CERT relies on the presence of dedicated trained team, which is called for the immediate handling of the event. The same team also reviews various aspects of security and safety as well as training and community awareness of protection methods.

The State has prepared and trained a local team capable of handling the various dimensions of security and integrity of information. This has begun in Q-CERT in 2006, and it is the only body that deals with emergency computing. Q-CERT has also equipped a dedicated team to educate and sensitize institutions and companies to the extent of risks facing them and the benefits they receive while cooperating with Q-CERT to reduce cyber risks.

The team of Q-CERT is also working with government bodies, public and private sectors authorities, and with Qatari citizens, to make them aware of the risks and threats they face on the internet. The team is also working to protect sensitive information on the internet and to guarantee its insurance.

3. International Forum for Incident Response and Security Teams

To combat issues of information security beyond the geographical boundaries of States, the Q-CERT team is a member of the international Forum of Incident Response and Security Teams known as "FIRST". This forum supports international relations that bind insurance teams to each other as partners around the world in order to exchange the latest information about threats and risks that are faced by sensitive websites.

4. Center for Combating Cybercrime

In 2006, the State of Qatar established one of the most important centers concerned with combating cyber crime in the Middle East; the Center of Combating Cybercrime, which follows the Ministry of the Interior. The State has taken measures to strengthen the ability of this center to perform its duties while combating cyber crime in all its forms. The center is not the first in the region, but it is characterized by the application and use of the latest equipment for combating this type of crimes. This is due to the great support given by the State for the development of all means to achieve security and safety for those who reside on the territory of the State of Qatar.

5. National Strategy for Cyber Security

Qatar has formulated a strategy that includes a number of initiatives that support each objective of the strategy of cyber security, and describes what measures the State of Qatar will take advance towards these goals. While the initiatives have been arranged in accordance with the goals, the initiatives are also objectives that could lead to progress and success in achieving other goals.

The strategy aims to achieve five goals: 1) the protection of the infrastructure of critical national information; 2) to respond to incidents and electronic attacks and help their resolution and recovery through the dissemination of information, and through cooperation in taking necessary actions; 3) forming legal and regulatory frameworks to enhance the safety and vitality of cyberspace; 4) to promote a culture of cyber security that will support the safe and appropriate use of cyberspace; 5) to develop and refine national strategies for cyber-security. Thank you.

President: I thank the distinguished delegate from Qatar for his statement. I now give the floor to the distinguished delegate of Pakistan.

The Delegate from Pakistan: Thank you, Mr. President. My compliments to the panelists for their succinct presentations. Pakistan respects the right to freedom of expression, but also believes that the right to privacy is a fundamental right, which is inviolable. While respecting the sovereignty of States, both territorial as well as subject matter, it is Pakistan's firm belief and commitment that no crime should go unpunished. Crime in cyberspace is a growing phenomenon: a concern for all nations, including Pakistan.

We in Pakistan have been working towards putting together domestic legislation in line with international standards. We would be happy to be part of a working group as suggested by the People's Republic of China's delegation. Thank you, sir.

President: I thank the distinguished delegate of Pakistan for his statement. I now give the floor to the distinguished delegate for the Democratic People's Republic of Korea.

The Delegate from the Democratic People's Republic of Korea: Thank you, Mr. President. Cyberspace is deeply infiltrating human life and giving greater impact to the political, economic, and cultural sectors. Such expansion of cyberspace has its contribution to social development, while on the other hand it brings about serious problems.

It has been noted that due to its unique features of no national boundary and transnational information flow, cyberspace has the risk to be abused to violate State sovereignty and national interests of each country. The United States, taking the advantage of its monopoly position in cyberspace is diverting the use of cyberspace from serving the sound advancement of humankind, and slandering and disturbing the social and political stability of other independent countries. Last year the US backed the dissemination of the movie entitled *The Interview* through the internet, which viciously falsified and dishonoured the social system of the DPRK, and thus extended its confrontation policy against the DPRK to cyberspace.

Another example of US infringement of State sovereignty: the US imputed the cyber attack on *Sony Pictures* to the DPRK without presenting any concrete evidence, and subsequently interrupted the internet connection to the DPRK homepage. Such violations in cyberspace are not limited to DPRK only. As Edward Snowden–a computer analyst–revealed, the US practices in cyberspace, such as the interception of email and other communications online, are disregarding whether the victim is the Head of State, its ally or hostility without any discretion.

The DPRK regards that State sovereignty should be definitely secured in the use of cyberspace and rejects all forms of cybercrimes on the internet. We call for eliminating all forms of illegal acts, including falsifying and dishonouring the social-political system of other countries under the pretext of freedom of speech and expression, and insists to guarantee the established principles of international law, such as the respect of State sovereignty, non-interference in internal affairs, right to self-determination, and international cooperation. The DPRK Government aspires to the sound and healthy development of cyberspace and will cooperate closely with AALCO Member States to prevent all forms of illegal activities and militarization of cyberspace. Thank you very much.

President: I thank the distinguished delegate of DPRK for his statement. I now give the floor to the distinguished delegate of Oman.

The Delegate from Oman:[3] Thank you, Mr. President, and thank you all speakers on this topic. As I mentioned yesterday, cyberspace is very important and it plays a pivotal role in the field of world trade, and in all walks of life. It is important for AALCO to give this topic utmost importance, and through the adoption of the AALCO resolution to prepare an international convention for the regulation of cyberspace, thus ensuring the use of this space for the service of all mankind, and also ensuring the secure transmission of information and the protection of human. Of course, States must not work towards depriving each other of these rights.

So, I repeat my request for the adoption of an AALCO resolution to create, issue, or adopt, an international convention to organize this and ensure the use of this area in the humanitarian sphere in peaceful manner and for the service of all humanity. Thank you very much.

President: I thank the distinguished delegate of Oman for his statement. Now I give the floor to the distinguished delegate of Sudan.

[3] This statement was delivered in Arabic. This is an unofficial translation made by the Secretariat.

The Delegate from Sudan:[4] Thank you, Mr. President. In the name of God, the most compassionate, the most merciful; At the beginning we clarify the vision of Sudan about the draft of the international law or international convention for the protection of cyber judicature, where Sudan supports the importance of adopting a proposal of this agreement as it represents the international legal framework. International law is not only important for the protection of inflammatory aspects but also represent a framework of cooperation to build confidence in the cyber judicature through: -

1. Security cooperation:
There is a need for all States to take measures to prevent and combat cyber crimes, including organized crime, terrorist cyber crimes, and money laundering.

2. Judicial cooperation:
Broadcasting confidence in cyber judicature requires judicial cooperation and that will be possible by providing necessary assistance for investigation and court proceedings.

3. Extradition:
The principle of extradition is a form of cooperation in the field of cyber judicature.

4. *Letters Rogatory*:
To project confidence in judicial cooperation, the importance of the agreement on the principle of *Letters Rogatory* is based on the easy reporting of judicial documents, hearings, implementation, and inspections.

The importance of identifying the institutional framework to follow up on cyber security matters

It is important that each State establishes a national council for safety and cyber security, as well as an independent supreme national body for safety and security in cyberspace.

There is an important need for international law to build confidence in cyberspace and a need to strengthen and promote that by concluding bilateral and regional agreements in the areas mentioned above, as well as a need for countries to adopt an integrated legal system at the national level. In this regard I cite examples of national laws adopted by Sudan in the field of the protection of cyber judicature, namely:

1- Communications Act of 2001
2- Electronic Information Act 2007
3- Informatics Crimes Act 2007
4- National Center for Information Law, 2010

Thank you.

President: I thank the distinguished delegate from Sudan for his statement. Dear colleagues, that comes to the end of my list of speakers on this item. Thus we have

[4] This statement was delivered in Arabic. This is an unofficial translation made by the Secretariat.

concluded this discussion on the item of "international law in cyberspace". Of course we are delighted that the discussion has attracted so much attention from Member States. I think this will be an enduring issue for AALCO to continue the discussion in future Sessions. On this occasion I would like to thank all the delegations for participating in this special meeting and also for their contributions. Particularly I would like to thank the two panelists, Mr. Fan and Mr. Desgange, for their presentations and for their participation in the discussions. I declare this special meeting adjourned. Thank you.

The meeting was thereafter adjourned.