Contribution of the Islamic Republic of Iran to the Global Digital Compact April 2023

1. Certain components of favorable vision for cyberspace:

The favorable cyberspace is a global ecosystem consisting of digital domains under sovereignty of the States and its entangled societal systems based on the regulated interactions of actors on the basis of independent, interoperable and manageable networks with the ability to apply sovereign rights of the States and the national jurisdiction of the countries, which has the following characteristics:

- 1. The favorable cyberspace has the ability to be designed, developed and managed on the basis of fundamental principle and rights for the good and happiness of humanity, the high and common interests of human societies and in the service of purely peaceful goals and being free from conflicts, crimes, deviations and harms;
- 2. The favorable cyberspace is lawful with the efficient and appropriate legal system and agreed fair, transparent and ethical principles and rules;
- 3. The favorable cyberspace is just and multipolar based on the fundamental principles of the international law that the sovereignty of the States is respected in its ecosystem and the digital sovereignty and balanced approach to the rights and duties of governments are recognized;
- 4. It has a new, multilateral, fair, non-discriminatory, transparent and responsible governance framework with the equal participation of all countries and a regulatory system with the approach of benefiting from the consultation of stakeholders, considering the leading role of the States in this field;
- 5. The favorable cyber space is secure, stable, safe and healthy, developmentoriented, neutral, peaceful, free from violence, trusted and is a platform for the growth of virtues for everyone as well as supporter of the stability, national security, national solidarity and coherence, and security, integrity and health of all national systems;

- 6. It is free from unilateral coercive measures as those measures are major obstacle in the decision-making system based on the sovereignty of the States, as well as an impediment in the way of the digital transformation of nations, or their benefits from global networks and the development of information and communication technologies. Likewise, barrier for the benefit of users from their rights in digital ecosystems;
- 7. Supporter of the decision-making system based on the national sovereignty of countries, supporter of social justice, driving force of productivity and economic prosperity, facilitator of transparency, public supervision and fight against injustice and corruption in all forms and manifestations;
- 8. Having responsible, capable users with valid digital identity, literacy and skills necessary for safe living in cyber ecosystems;
- 9. It has fair distribution of digital resources and benefits resulting from global networks and information and communication technologies;
- 10.It has Balanced, two-way, and regulated circulation of useful, valid and reliable information, while it has local and context based content moderation systems for harmful and illegal content against individual and society in consistence with national law and values;
- 11.In this space the fundamental national rights and values are guaranteed, the right of digital self-determination and the right to development of countries are recognized, and all countries have the right to determine their own model of development and governance in this new ecosystem in a fair and equal manner;
- 12.It has efficient, fair and transparent framework of accountability and responsibility for all the actors (in particular, accountability of powerful and influential actors, including cross-border service providers according to the laws and regulations of the country where they have digital presence, effect and activity);
- 13.It has safe, trustworthy, flexible and interactive infrastructures within the framework of technical and security standards accepted by all the governments;
- 14.In the favorable cyber space, the countries respect each other s rights in choosing their own model of development, governance, regulations of cyber space and public policy concerning the internet issues. States have

right to operate own cyber space in line with their national law. They have jurisdiction on infrastructures, data, resources, services and related activities to information and communication technologies in their own territories. Likewise, they have right to protect of their civilians, systems and digital resource against threats, crimes, damages, disruptions, crossborder attacks, subversion and foreign interference to defend their own rights, fundamental values and legitimate interests in cyber space;

- 15.In the favorable cyber space, no country should seek digital dominance, colonialization and unilateralism. No country should use cyber space, the internet and communication and information technologies for intervention in the domestic affairs of other countries, or should not support or participate in the cyber activities that undermine the security, sovereignty and stability of other countries, by misusing its superiority in the cyberspace;
- 16.All countries should enjoy necessary capacities and tools for exercising sovereignty in the cyber space in order to manage possible risks and harms caused by the global networks and services provided on their platform, and should protect all societies particularly children, women and families visis negative effects and consequences of cross-border illegal, criminal and harmful contents and activities in the internet, digital platforms and emerging virtual environments including Metaverese;
- 17. The favorable cyber space enables the digital economy in a balanced, safe, comprehensive and multilateral manner;
- 18.Protecting and expanding cyber space in the favorable one, respect environment and safeguard the environmental assets of the countries;

2. Connecting all people to the internet, including all schools

- 1. Regular, Safe, fair, free, reliable and affordable access to all communication resources and cross-border data flows under the national rule and laws;
- 2. Secure, Sustainable, resilient, stable and regulated global networks consisting of public digital infrastructure and independent and

interoperable networks (under the sovereignty and management of the governments) based on rules and protocols agreed upon by all the countries;

- 3. Global networks should be reliable, peaceful and development oriented, and connection to the global networks should not mean the entry of citizens or businesses or governments into the new arena for creating conflicts and expanding battlefield;
- 4. Fair distribution of resources and opportunities of connectivity and digital inclusion, so that the existing gap between the north and south countries should be prevented and reduced;
- 5. Respecting to principles, values, high interests, the national identity system, ethical and moral standards and cultural sensitivities of nations and values of global religions, by all the active players in cyber space and ecosystem of internet governance, including in the field of international cooperation;
- 6. Respecting sovereign right of the States in choosing digital development model and determining policies in the field of connectivity and access and management model for access with regard to local context based on domestic laws;
- 7. Respecting and protecting cultural diversity, linguistic diversity and local content in the international cyber space;

2-1-2- Actions and Commitments for realization of the Principles

- 1. Strengthening international cooperation in the digital capacity building filed based on priorities and needs of the recipient countries, in a nondiscriminatory manner and without intervention in the domestic affairs of the countries and compatible with their economic and social conditions;
- 2. Joint efforts to create multilateral, fair and transparent governance system with equal participation of all countries in their important and strategic decisions of global networks including the internet;
- 3. Setting internationally agreed rules and regulations by all States in the area of providing and using of services of satellite internet and activities of providers of all connectivity and access services to global networks, including satellite systems in respect to sovereignty of States and in consistence with requirements and law of recipient countries;

4. Ensuring necessary political and legal guarantees by key players including dominate States and institutions over global networks and services provided on their platforms for non-abuse of them to realize the illegitimate goals and illegitimate interests including:

-Non-application of discriminatory policies and unilateral coercive measures by the governments and institutions that have dominance, monopoly and authority over the infrastructure, technology, services and vital resources of global networks and the internet;

-Inclusive connectivity to global networks and access to services provided in their platforms should not become a tool for systematic violation of national sovereignty and intervention in the internal affairs of States;

-Inclusive connectivity to global networks and access to services provided in their platforms should not damage national stability and security and undermining security and stability of economic, social and cultural systems of countries;

-Inclusive connectivity to global networks and access to services provided in their platforms should not be used as a tool for leading and organizing chaos and insecurity, inciting violation through organized dissemination of disinformation and hate speech campaigns against countries and religions;

5. Improving international cooperation in exchanging technology, knowledge and experience in the field of information and communication technology in a non-discriminatory manner, with regard to the effects of digital space on all legal, political, civil, economic, social and cultural aspects;

2-2 - Developing Digital Education based on Justice and Values

1-2-2- Fundamental principles

- 1. Providing safe, fair, free, legal and reliable access to useful and trustworthy educational resources for all ages and languages;
- 2. Creating global networks of scientific content and knowledge based, consisting of independent sub- networks under the governance and management of governments and interoperable on basis of the rules and protocols agreed by all countries;

- 3. Empowering, educating and training users in a proper way for a healthy and safe life in cyber space based on principles, values and educational principles governing the official education system of countries;
- 4. Respecting and protecting cultural diversity, linguistic diversity and local content in international digital environment;
- 5. Non-application of discriminatory policies and unilateral coercive measures by the governments and institutions that have dominance, monopoly and authority over content provided on scientific global networks;

2-2-2- Actions and Commitment for Realization of Principle

- 1. Strengthening international cooperation in the exchanging knowledge, technologies and best practices in the field of development of digital education in a non discriminatory manner;
- 2. Formulation and implementation of the national digital transformation programs in the field of education with the aim of establishing educational justice, inclusive education with quality and lifelong learning, based on the model of local development programs, values, policies and the roadmap of the national education system in all elementary, secondary and vocational levels;
- 3. Establishing appropriate and efficient framework at local level for digital training in certain fields including: investment, infrastructures, networks, products, contents, services and digital systems and creating special protected, healthy and safe environments for children and students;
- 4. Implementing national programs for improving literacy and digital skills for schools, with the aim to train responsible, capable users with appropriate skills for digital ecosystem and to provide safe and equal participation in the society and in the digital economy and to prevent and fight against all forms and manifestations of emerging risks, crimes and damages of the digital ecosystem;
- 5. Prohibiting unilateral coercive measures in the cyber educational space with the aim of fully realization of international cooperation and interactive with relevant institution and non-blocking of IP address of countries due to compliance with of unilateral sanctioned imposed by certain countries;

6. Free and non- discriminatory access to online platforms by educational and scientific community for participation in online educational meetings and workshops including virtual meeting of the UN as well as non- applying restrictive in access to information, education and scientific bases;

3. Trust and Internet Fragmentation

- 1. The applicability of a wide range of principles of international law in cyberspace, including the principle of equality of sovereignty, refraining and prohibiting the use of force, and non-interference in the internal affairs of other countries in and by using cyberspace;
- 2. Guaranteeing, respecting and safeguarding the sovereignty of member states in all layers and dimensions of cyber space (in the field of infrastructure, data, digital resources, services, information, content, process, users);
- 3. The principle of respect for independence and the right to digital selfdetermination of countries and right to determining model for digital development;
- 4. Respecting the right of countries for development and the right to select the model for governance on digital ecosystem and regulatory system in the jurisdiction of countries and within the framework of national laws, for the protection of public rights and interests;
- 5. Negation of all manifestations of digital colonialism and unilateralism in all layers of cyber space;
- 6. Following shared interests and real multilateralism in internet governance by promoting the role of governments and improving consultations with all multi-stakeholders and creating transparent, accountable, democratic international internet management system with the equal participation of all countries and dealing with monopolization in its management;
- 7. Equal participation of countries in governance and decision-making process related to international cyber space and internet management, based on common obligations and responsibility of all member states for materializing the favorable vision(while according the paragraph 69 of the Tunis Agenda there is need for enhanced cooperation to enable governments to carry out their roles and responsibilities, in international

public policy issues pertaining to the Internet, the enhanced cooperation has yet to realize);

- 8. Geopolitical neutrality of the internet during international crisis and conflicts and preventing misuse of information and communication technologies and prohibition of using the Internet and cross-border digital platform as a weapon to achieve illegitimate geopolitical goals;
- 9. Internationalization of the public core of the internet as a global public goods;
- 10.Shaping fair cyber order and smart, efficient and proper law system to entail all interactions in all layers and main organs;
- 11.A peaceful goals and application, violence-free cyber space (only peaceful goals and objectives), promotion of stability and security in using ICTs with emphasize on prevention of cyber hostilities and harmful and peace-threatening activities, international stability and security and peaceful settlement of international disputes;
- 12.Necessity of accountability of cross-border platforms before users, public and the regulatory system of countries and transparency of their processes, performance and digital presence while respecting the laws and values of societies;
- 13.Not to follow the policy of cultural assimilation and imposing their values and lifestyles on other societies by dominant countries in the cyberspace and supporting cultural diversity and multilingualism on the internet;
- 14.Observing the concerns and national interests of all countries in a balanced manner in the process of development, governance, norms, rules and standards setting of the global digital ecosystem;
- 15.Enabling equal digital development for all countries;
- 16.Effective international cooperation for dealing with international challenges related to cyberspace;

3-2-Actions and Commitments to Realization of the Principles:

- 1. Supporting the favorable vision and architecture of cyber space by Global Digital Compact that are mentioned in this text;
- 2. Collective and dedicated efforts to materialize needed treaties in order to regulate fair and balanced international relations in the cyber space, including the comprehensive convention on cyber security and information

and communication technologies and setting of the comprehensive convention against the use of ICTs for criminal purposes;

- 3. Collective efforts for creating governance framework for cyber space and internationalization of internet management within the framework of United Nations based on genuine multilateralism and consultation with relevant stakeholders as well as justice, ethic-centered, political neutrality and other principles and norms accepted by all countries, based on considering respect for the legal system and national laws of countries;
- 4. Providing comprehensive and obligatory framework for the responsible behavior of countries in the cyberspace, taking into account the opinions and concerns of all member countries;
- 5. Collective and dedicated efforts for determining and creating the mechanism of effective cooperation of the member States in providing the global framework of principle, norms and rules governing the accountability of cross-border digital platforms to governments and users (in the fields of data protection, dealing with criminal and harmful content, legal representative and competition and ...)
- 6. Creating necessary framework for strengthening needed arrangements, regulations, capacities and capabilities in order to apply national sovereignty in the cyber space;
- 7. Creating technical-legal system of independent and interoperable networks (designing the framework of interaction and cooperation among national information networks of the countries within the framework of a new architecture);
- 8. Reforming the management of names and domains mechanism as well as internet public resources and infrastructures in the context of equal participation of all countries with the aim of managing harms and risks, fighting against cybercrimes and ensuring online safety;
- 9. Creating the system of responsibly for all states vis-Ŀvis the behavior of big technology companies and owner of cross- border digital platforms registered in their countries, and obliging them to respect the rights of users, national sovereignty of other countries, and compliance with the laws and regulations of the countries in which they have digital presence, activity and influence;
- 10.Making the efforts to establish digital identity system in the national and international level, while respecting the national law of service recipient countries;

- 11.Creating necessary frameworks for guarantee the ethical, human, cultural and social considerations in the process of designing and developing digital ecosystems, technology, innovations and digital services;
- 12.Creating necessary frameworks for protection and safeguarding the sovereignty of the countries in cyber space and the right of countries in choosing the model of digital development and cyber space governance based on national laws and values;
- 13.Recognizing and guaranteeing the right of countries for development in the cyberspace and the need for prevention of unilateral coercive measures (UCM) against with the sovereign rights of the States and human rights, by certain Sates, technology companies and cross-border digital platforms;
- 14.Collective, inclusive, fair, non-discriminatory and affordable access and usage of ICTs as well as in their managing and governing should be assured in respect to national conditions;
- 15.Setting principle, norms and rules for responsible behavior of global digital platforms, including the requirement to establish a legal office by cross ت border digital platforms in countries that they have influential presence and high penetration among users;
- 16.Exploring the cooperation opportunities in the field of designing and creating joint regional digital platforms;
- 17.Creating Data Bank regarding cyber laws and regulations of the countries, in order to inform all beneficiaries about the legal conditions of the countries;

4. Data Protection

- 1. Respecting national data sovereignty, data localization, storage of citizens' data and digital sovereignty of the States;
- 2. Considering legal processing, usage and sharing of data;
- 3. Protection of countries udigital assets (including cultural and civilization heritage in the field of digital content, big data and a)
- 4. Developing regulated, trusted cross-border data flow, taking into account the considerations of data protection, security and national digital economy and the requirements of digital innovation and development;
- **5.** Observing justice and fairness in access to benefits and advantages of digital data;

- **6.** Facilitating digital trade while ensuring safe and secure data economy with respect to privacy and protection of data within the framework of domestic laws and regulations of the countries;
- 7. Increasing trust in the digital economy;
- 8. In using personal data by providers of services, they should respect fairness and transparency principles, legality of services accordance with national laws of services recipient countries and proportional with defined objectives for their services and observing adequate and time limitation of providing services and informing data owners on using their data;
- **9.** Respecting national sovereignty, requirements of countries over their data of users in the area namely, sharing data, transferring data to other countries, national data, hosting and place of storing data, protection of sensitive data and big data;

4-2- Actions and Commitments to realization the Principles

- 1. Providing international legal frameworks in the field of data governance, data security and regulated and trusted cross- border data flow, with respect for the principle of data sovereignty by the States in the global information space including the formation of a global data treaty with aim of countering against misuse of data for illegitimate political and economic goals, assisting global challenges and supporting national priories (in the area including, sovereignty, security, governance, exchange, property rights and data economy, etc.);
- 2. Countering against dominant role of certain cross border digital platforms;
- Providing international indexes and reports regarding respect for the users rights in the cross-border digital platforms;
- 4. Obliging technology companies and cross-border digital platforms for respecting laws of the countries in privacy and data governance;
- 5. Reinforcing the main role of the United Nations in promoting a more balanced global data governance with the aim of benefiting all countries from the advantages and benefits of data and countering against the spread of injustice in this area;
- 6. Strengthening international cooperation mechanisms in the arena of developing infrastructures and capacities to create, store, secure and absorb

value from raw data in order to use data as a new economic resource is needed;

7. Data and data flows can support the development of various solutions to global development challenges which for realizing, needs enhance international cooperation, technology transfer and capacity building as well as strengthening the capacities of the developing countries to harness data for achieving national development goals and having an equal participation by them in the data value chain;

5. Applying Human Rights Online

- 1. Adhering the natural and divine nature of human rights, human dignity, cultural diversity, the family, development, justice and equality before the law and non-discrimination, the right to freedom in accordance with the law and the right to security as fundamental values;
- 2. protecting rights and legal and responsible freedom in digital ecosystem according to constitutional laws of countries and international commitments agreed by all countries, while protecting public rights, national security, public security, safety, health, ethical and respecting other srights (particularly by cross-border digital platforms);
- 3. Supporting and strengthening the approach towards respect for cultural and ethical diversities among societies in regard to internationally agreed human rights principles and taking into account their characteristics in the cyber space;
- 4. Safeguarding the public rights and protecting privacy for digital communication, ensuring data protection at national, local and individual levels along with safeguarding national security at digital arena;
- 5. Sticking balance between individual rights and freedoms and public interests in digital ecosystem;
- 6. Universal and non-discriminatory access to information and communication technology and to their advantages and interests in the cyber space by all nations are necessary;
- 7. Free and fair access of all people to the reliable and valuable knowledge, information and services for the growth of individual and society including scientific proposes based on national security and protecting the rights and interests of society and people;

5-2- Actions and Commitments for Realization of Principles

- 1. Providing necessary frameworks for identifying, pursing and countering against systematic violence of users rights in digital ecosystem including social media and international digital platforms;
- **2.** Developing principles, norms and regulations governing human rights commitments and obligations of technological companies and owners of cross-border digital platforms within the framework of UN.
- **3.** Forming normative frameworks to remove unilateral coercive measures in the cyberspace that prevent countries to access benefits of new communication and information technologies and global networks as a main barrier to achieving national digital development and violation of rights of nations;
- 4. Developing internationally agreed indicators and reports by all countries regarding the observance of the rights of users in cross-border digital platforms;

6. Introducing Criteria for Accountability for Discriminatory and Misleading Content

6-1- Fundamental Principle

- 1. Accountability of cross-border platforms before users, public and regulation system of countries and their responsible digital presence while respecting national laws and values;
- 2. Respecting national fundamental values, cultures and local sensitivities;
- 3. Striking a balance between the rights and legal freedoms and the protection of society against harm and ensuring safety, health and psychological security of users on the Internet and online environments;
- 4. Respecting the transparency of procedures, algorithms and functions of cross-border digital platforms (regarding respect for user s rights, public rights, public safety, national security, morality, security of systems, content health, safety of platform, policies of content moderation, cooperation with law enforcement and judicial authorities to prevent and combat ICT-dependent and ICT-enabled crimes);

6-2- Actions and Commitments for Realization of Principles

1. Regulating framework of digital platforms with management and content moderation approach based on local laws, culture and values with the aim to ensure users safety in online space and protection of societies

concerning negative effects resulting from illegal, criminal and harmful content, while safeguarding legal rights and freedom;

- 2. Setting appropriate laws at the national and regional level regarding the prevention and fighting against illegal and harmful content on the Internet and cross-border digital platforms and determining the requirements, obligations and guarantees of their implementation in this regard;
- 3. Providing accountability system for governments on illegal function and behaviors of big technological companies which are registered in their territories and owners of cross-border digital platforms and their obligation regarding respect to the rights of users, national sovereignty of other countries and following up of laws and regulations of the countries which are active and have digital influence;
- 4. Providing the system of accountability for those who provide cross- border digital services, determining the obligation of platforms, search engines, emerging virtual environments based on the new generation of web and artificial intelligence such as Metaverse regarding the creation of legal representation, cooperating with competent national authorities and coping and preventing criminal, illegal and harmful actions and content (including child abuse, fake news, disinformation, spreading hate, incitement of violence, forgery and fraud, online harassment and Δ Δ.)
- 5. Making the efforts for adopting preventive measures particularly for commercial companies relating to digital space for fighting against dissemination of disinformation and fake news regarding historical territorial, social, cultural, geographical identities of states and falsification of their territorial and historical realities;
- 6. The requirement to have a legal operation and to establish official representation for cross-border digital platforms in countries that are influential and have a high penetration rate among their users;
- 7. Criminalization of providing access, recommending and sharing all forms and manifestations of illegal and harmful content to children and teenagers, including, obscene content, pornographic materials, child sexual abuse martials, encouraging suicide, any content encouraging sexual deviations, promoting and normalizing incest and adultery, self-torturing and sadism and other sexual violence against women in national law and cybercrime conventions;
- 8. Determining the criminal responsibility of the owners of cross-border digital platforms regarding harmful content, services and algorithms and

the lack of essential cooperation with the competent national authorities regarding countering against criminal and harmful acts and content and criminalizing the misuse of digital tools by the owners of digital platforms for illegal intervention violating national sovereignty and undermining stability, national security, public order and ethics in other countries by leading and organizing insecurity and chaos in other countries by not confronting or helping the organized dissemination of disinformation and hate speech campaigns and incitement to online violence via using algorithms based on artificial intelligence;

- 9. Criminalization of insulting the sanctities and values of divine religions and publishing defamatory and untrue content with the aim of destroying and tarnishing of divine religions, their leaders and followers on the Internet and digital platforms;
- 10.Making collective cooperation between governments and owners of technology companies in the field of fighting against organized xenophobia, promoting racism and destroying the image of nations and religions on the Internet and international digital platforms;

7. Improving the Regulation of Artificial Intelligence

- 1. Fundamental principles of international laws and principles and objectives, enshrined in the UN Charter in the development and deployment of AI;
- 2. National sovereignty in providing data required for technologies and artificial intelligence systems;
- 3. Protecting users, rights and fundamental national values in the design, development and governance of artificial intelligence;
- 4. Legal and legitimate purposes and peaceful uses of artificial intelligence;
- 5. Health and safety in artificial intelligence design and development;
- 6. Designing and development of artificial intelligence based on values and moral considerations;
- 7. Accountability and responsibility of designers, developers, organizers of products and services of artificial intelligence;
- 8. Responsible innovation and non-harm to others, especially in the field of artificial intelligence;
- 9. Transparency and ability to explain algorithms;
- 10. Non-bias approach in possesses, outputs and in decision-making of artificial intelligence-based systems;

- 11.Not entrusting fateful decisions and related to life and death to artificial intelligence systems;
- 12.Multilateral governance of artificial intelligence with participation and consultation of other stakeholders;
- 13. Prohibiting the production and proliferation of fully lethal autonomous weapons systems by using artificial intelligence, with lack of control and responsibility of the human agent and contrary to the ethical principles and rules of international law;

7-2- Actions and Commitments for Realization of Principles

- 1. Providing necessary frameworks for development and promotion of digital ethics based on values and legal and ethical frameworks of countries for designing, development, governance and use of ICTs in particular, emerging technologies and with participation of States and leaders of religions for forming reliable and ethical AI ecosystem;
- 2. Development of an appropriate international legal framework in development and application of artificial intelligence;
- 3. Artificial intelligence developers should anticipate any unwanted deviation of the artificial intelligence towards criminal and harmful actions and provide the necessary control and prevention tools. These control tools should be explained to operators and users and made available to them.

8. Digital Commons as Public Goods

- 1. Digital fairness and justice (removing injustices and the digital divide in individuals and nations' enjoyment of advantages, opportunities, resources, systems, services, legal content, regardless of religion, ethnicity, nationality, gender, race within the framework of laws and values of societies);
- 2. Internationalization of pubic core of internet as a global public goods;
- 3. Respecting for independence and digital right of self- determination of countries determining model for digital development;
- 4. Respect for the right of countries for development and the right to determine the governance model in digital ecosystem and regulatory

system in the field of judicial competency of the countries and within the national laws for the safeguard of public rights and interests;

- 5. Avoiding unilateral coercive measures which prevent the realization of economic and social development for the population of effected countries and prevent them from fully benefiting of the advantages and benefits of communication and information technologies;
- 6. Confronting technological monopoly as an element which prevent the growth of industry and digital development of all countries, particularly emerging countries in the process of technology;

8-2- Actions and Commitments for Realization of Principles

- 1. Recognizing and guarantee countries right to development in the cyber space and the necessity of confronting technology sanction and unilateral coercive measures against human rights ((in the fields of investment, infrastructure development, connectivity and access, digital resources, Hardware and software needed for digital development and transformation) adopted by governments and digital platforms;
- 2. Creating governance framework and regulating digital joint affairs with emphasize on the principle of: safeguarding privacy, data, transparency cultural diversity within the framework of national laws and values and avoiding monopoly;
- 3. Establishing a governance framework and setting regulations regarding digital commons with an emphasis on the principles of privacy and data protection, transparency and accountability, avoiding concentration and monopoly, cultural diversity within the framework of national laws and values;
- 4. Designing and implementing of capacity building programs in the cyber field, including through digital commons, should be based on national development goals, national programs and needs of governments and in accordance with the economic, social and cultural situation, and should not use as a tool for interfering in their internal affairs;
- 5. Removing structural impediments of investment in the development of digital infrastructures and services, access and transfer of technologies and services needed for national digital transformation, as well as including unilateral coercive measures;

6. Creating institutional mechanisms for dialogue and knowledge- sharing, expertise, experiences and digital technologies among countries at the international level;

9. Other Areas:

9-Digital Security and Trust

- 1. Respecting sovereignty of governments in cyber space and nonintervention in domestic affairs of governments through cyber space and non-intervention in cyber domestic affairs;
- 2. Prohibition of threats or use of force against the territorial integrity and political independence of countries, including the prohibition of threats or use of force in and by cyberspace;
- 3. Mutual respect in international relations, and peaceful coexistence in the digital ecosystem and seeking fair pacifism;
- 4. Peaceful cyber space free from violence (objectives and uses based on peace), promotion of stability and security in using ICTs based on prevention of cyber conflicts and harmful activities that threaten international peace and stability, and settlement of international disputes through peaceful means;
- 5. Realization of the principle of cyber security for all (failure to secure oneself by violating the security of others);
- 6. The right of countries to comprehensively defend their cyber territory against all kinds of cyber threats based on the scale and severity of the effects of cyber operations on the country's critical infrastructures.
- 7. Geopolitical neutrality of the internet in international crises and conflicts and prevention of misuse of information and communication technology and use of internet and cross-border digital platform as a weapon to achieve illegitimate geopolitical goals;
- 8. Inclusive protection of societies before threats, crimes, cyber hostilities and harms resulted from illegal activities and content, threatening and weakening security, stability, safety, interest and values of countries;
- 9. Prohibition of production and use of fully lethal automatic weapons by using artificial intelligence which is contrary to moral principles and rules of international law;

- 10.Increasing the confidence of countries regarding the use of the Internet and information and communication technologies;
- 11.Designing and developing based on safety and security requirements (Security and Safety by design);
- 12. Transparency, trace ability and digital documentation;
- 13.Increasing transparency and reducing the misuse of anonymity in cyber space with the aim of preventing abuse and dealing with the use of ICT for criminal purposes (designing an internet architecture based on security and safety);
- 14. The need for governments to be responsible and accountable for the illegal behavior of their respective cross-border digital platforms in the information spheres, regarding creating and fueling insecurity and instability in other countries and incitement to violence through the organized dissemination of disinformation, criminal and harmful content (registered in its territory and licensed to operate);
- 15.Joint responsibility of governments particularly the governments having domination on technology and infrastructure, for providing security and safety for digital ecosystem, based on respect for sovereignty and security of the countries;
- 16.Adhering to technical, legal and related considerations in the complex process of attribution in cyber incidents;
- 17.Protecting national critical infrastructures against cyber threats and ensuring supply chain security;

9-2- Actions and Commitments for Realization of Principles

- 1. Strengthening a global committed effort to promote international cooperation for counting against cybercrimes and threats through shaping fair and balanced needed treaties to regulate international relations in the cyberspace, including the comprehensive convention on cyber security information and communication technology and establishing criminal justice by forming the comprehensive convention for fighting against the use of ICT for criminal purposes;
- 2. Creating international legal mechanism for prevention and peaceful settlement of inter-governmental disputes in global cyber space;

- 3. Development of commitments, standards and necessary capabilities for ensuring the security of vital national infrastructures vis-±vis cyber threats and to ensure supply chain security;
- 4. Development of new principles and norms of current international rights and completing balanced and obligatory framework regarding the moral and behavior of member states in global cyber space, by taking into consideration the views, interests and concerns of all member states;
- 5. Preventing and countries against the use of information and communication technology for criminal purposes and effective international cooperation in the field of seeking and pursuing cybercrimes, including the exchange of information and digital evidence;
- 6. Preventing, managing and effectively countering against all verities of criminal and harmful actions and content in the cyber space with the aim of ensuring the safety of users and comprehensive protection of the rights, interests and values of societies, including maintaining stability, public order and security, cultural and civilizational identity, safety and public health and public morality in online environments;
- 7. developing common standards and procedures for exchanging digital evidences for seeking and pursuing cyber -crimes;
- 8. Creating the necessary mechanisms to communicate the judicial authorities of all countries through an online platform, structured, safe, secure, fast, integrated and accessible to the competent authorities of all countries;
- 9. International cooperation in dealing with the Dark Web and anonymization networks as an enabling environment for all kinds of illegal activities and organized crimes;
- 10.Creating necessary frameworks for safeguarding and protecting the sovereignty of the countries in cyber space and the rights of the countries in choosing the model for digital development and the governance of cyber space based on national laws and values;
- 11.Preparing an effective cooperation framework among the custodians of the internet governance ecosystem as well as the guardians of the IP and management system with law enforcement and judicial authorities of the countries in the prevention and fight against cybercrimes;

10.Cultural – Social

- 1. Respecting principles, values, interest, national identity, ethical criteria and cultural sensitivities of world religions, by all players who are active in cyber space and ecosystem of internet governance;
- 2. Empowering users and giving them appropriate training for safe and healthy existence in cyber space, based on principles, values and educational foundations of societies;
- 3. Protecting the values of the holy institute of the family as a fundamental unite of society and maximum protection for children and respecting their rights in online space within the framework of national laws and treaties agreed by each country;
- 4. Ethic and morality oriented approach in the internet and respect to cultural-social considerations of the countries in the development of infrastructure, content and services;
- 5. Respect for cultural diversity, linguistic diversity and native content in the context of information society and international cyber space;
- 6. Safeguarding digital cultural heritage of the nations and also the national identity elements in cyberspace and emerging virtual environments;
- 7. Guarantee safety and health and harm prevention in digital ecosystem (in the contents, services, infrastructures, websites, tools);
- 8. Not causing harm and damage to others in or through cyber space and virtual environment;
- 9. Taking into account the ethical aspects of information and communication technology and other aspects of cyber space;
- 10.Responsible innovation based on ethical values and not harming others, especially in the field of artificial intelligence;
- 11. Taking notice on special social groups including children, youth, elders, physical and mental disabled people;
- 12.Protecting environment by using information and communication technology;

10-2- Actions and Commitments for Realization of Principles

- 1. Providing necessary frameworks to guarantee respect for humanity, ethical, moral, cultural and social considerations in designing and developing digital ecosystem, technology and innovation;
- 2. setting program for promoting countries capacities in the field of production and dissemination of native contents with the aim to preserve

and promote cultural and civilizational identity and heritage of the member countries in the platform of cyber space;

11.Digital trade and Economy

11-1- Fundamental Principles

- 1. Regulated, trusted cross-border data and information flow, respecting sovereignty considerations including data sovereignty, national digital security and economy;
- 2. Avoiding unilateral coercive measures that prevent the people of targeted countries from full realization of economic and social development and deprive them from fully benefiting from the advantages and benefits of information and communication technologies;
- 3. Net neutrality with the aims of creating a level and fair playing field for the development of innovation and create equal parts for start-up companies and digital entrepreneurs (having equal behavior in the networks regarding access to website and services, based on equal opportunities for newly established companies and entrepreneurs);
- 4. protecting competition and the rights of producers and consumers of goods and services in the cyberspace at the national and international levels;
- 5. Benefiting from a valid digital identity within the framework of national laws and regulations;
- 6. Fair and inclusive multilateral governance in the field of cross-border digital economy and trade, based on multilateralism and fair and transparent governing rules accepted by all countries;
- 7. Facilitating digital commerce while ensuring a safe and secure data economy, and respecting privacy and data protection within the framework of domestic laws and regulations of countries;
- 8. Protecting the workforce, consumers and businesses in the field of digital economy and business;

11-2- Actions and Commitments for Realization of Principles

1. Creating independent and interoperable digital markets, while respecting the rights of the countries in regulating to achieve the objectives of public policies and respect for national requirements and regulations of digital markets at national and international levels, by the foreign actors;

- 2. Creating an enabling environment for safe, secure, healthy, trusted digital trade, while respecting the national sovereignty of countries;
- 3. Legal and responsible activity of cross-border digital platforms in financial, commercial and economic fields in the area of territorial jurisdiction of other countries;
- 4. Collective collaboration for the setting and developing international principles, norms and rules to counter effectively against anti-competitive practices of big tech companies in the digital ecosystem, and also for abuse of technological companies from their dominant position to eliminate competitors and impose unfair and unilateral conditions on other actors;
- 5. expanding digital entrepreneurship and strengthening relevant regulatory frameworks;