Sovereignty in Cyberspace: Theory and Practice

(Version 2.0)

Jointly Launched by
Wuhan University
China Institute of Contemporary International Relations
Shanghai Academy of Social Sciences

Jointly Released by
Chinese Academy of Social Sciences
Tsinghua University
Fudan University
Nanjing University
University of International Business and Economics
Cybersecurity Association of China

Throughout the history of world civilization, the meaning of national sovereignty has changed and been enriched over time. Humanity has successively undergone agricultural, industrial, and information revolutions, which have had enormous and profound impacts on the connotation and denotation of national sovereignty. In the agricultural age, human activity was mainly confined to land, so the focus of national sovereignty was on protecting territorial integrity. In the industrial age, human activity extended from land to the sea and sky. The scope of national sovereignty expanded accordingly. Highly integrated with the physical space of human activity in the information age, cyberspace has become a new frontier for modern states and a new domain of global governance. It is from this that sovereignty in cyberspace has emerged.

Sovereign states are key actors in carrying out activities and maintaining order in cyberspace. The principle of sovereign equality enshrined in the Charter of the United Nations is a basic norm governing contemporary international relations. Covering all aspects of state-to-state relations, its principle and spirit also apply to cyberspace. In practice, all countries have extended national sovereignty to cyberspace, but different understandings exist around the ideas and practices for exercising it. To facilitate more just and equitable global Internet governance and build a community with a shared future in cyberspace, the international community should, with the common well-being of humanity in mind, follow and practice the notion of sovereignty in cyberspace in line with the principles of equal consultation and seeking common ground while setting aside differences.

The Concept of Sovereignty in Cyberspace

I. Rights

Sovereignty in cyberspace is the extension of national sovereignty to cyberspace. It is the supremacy and independence that a state enjoys, on the basis of its national sovereignty, over cyber infrastructure, entities, behavior as well as relevant data and information in its territory. Specifically speaking, it primarily includes the following rights.

● **Independence.** A sovereign state has the right to independently choose its own path of cyber development, model of cyber governance, and Internet public policies, free from any external interference.

● **Equality.** In line with the principle of sovereign equality enshrined in the UN Charter, a sovereign state has the right to participate in global governance in cyberspace on an equal footing and jointly formulate international rules.

● **Jurisdiction**

• Legislative Jurisdiction. A sovereign state has the right to enact legislation to regulate cyber infrastructure, entities, behavior as well as relevant data and information in its territory, in order to protect its national security, public interests, and the legal rights and interests of its citizens, legal persons, and other organizations.

• Administrative Jurisdiction. A sovereign state has the right to administer cyber infrastructure, entities, behavior as well as relevant data and information in its territory according to law, so as to maintain good order in cyberspace.

• Judicial Jurisdiction. A sovereign state has the right to exercise judicial jurisdiction over cyber infrastructure, entities, behavior as well as relevant data and information in its territory according to law.

A sovereign state has the right to exercise, in accordance with the universally recognized principles of international law, necessary and reasonable personal, protective and universal jurisdiction over specific cyber activities outside its territory that have genuine and substantial connection with it. For smooth enforcement of such jurisdiction, it may seek assistance from relevant countries and regions in the spirit of self-restraint, comity and reciprocity.

● **Cyber-defense**

A sovereign state has the right to conduct capacity building on cyber security and adopt lawful and reasonable measures under the framework of the UN Charter to protect its legitimate rights and interests in cyberspace from external infringement.

II. Obligations

Whether in the physical world or cyberspace, sovereignty incorporates both rights and obligations. The connectivity and interdependence among countries in cyberspace all the more requires countries to respect the basic norms and general rules of international law and earnestly fulfill their due obligations specified in international law while enjoying the rights derived from sovereignty in cyberspace.

● **Non-infringement on other countries.** No country shall without permission access the critical network infrastructure or cyber systems closely related to another country's sovereign, security and development interests, or engage in acts of cyber surveillance, theft or sabotage.

● **Non-interference in other countries' internal affairs.** No country shall interfere in other countries' rights to survival, security and development in cyberspace, or their rights to maintain cyberspace order, security and development.

- **Due diligence.** No country shall knowingly allow its territory, or territory or Internet facilities, data and information under the control of its government, to be used for cyber activities undermining national security or interests of other countries.

- **Protection.** All countries have the obligation to protect lawful rights and interests of relevant cyberspace entities within their jurisdiction. They also have the obligation to promote openness and freedom of cyberspace while ensuring its order, security and development.

Manifestations of National Sovereignty in Cyberspace

National sovereignty extends to cyberspace, and is embodied through state activities in three aspects, namely Internet facilities and operation, Internet data and information, and society and individuals.

I. State activities concerning Internet facilities and operation

A state manages and uses Internet infrastructure in its territory to support system application, data and protocols on information dissemination; a state safeguards the security of Internet infrastructure and systems in its territory and protects them from illegal disruption or intrusion; a state participates in international cooperation on governance, development and utilization of Internet infrastructure and systems.

II. State activities concerning Internet data and information

A state guides, coordinates and protects the dissemination of Internet information in its territory and restricts the spread of information that infringes upon others' lawful interests or undermines social interests; a state bans Internet information that threatens public security being fabricated, distorted or spread in its territory by overseas organizations; a state participates in international coordination and cooperation on cross-border data flow, information governance and Internet information industry development; a state protects lawful Internet data and information from acts of infringement and protects the Internet data and information that involves national secrets from being stolen and destroyed.

III. State activities concerning society and individuals

Society and individuals refer to the social environment and actors that have impact on each other in cyberspace. The activities include the following. A state independently manages interactions between its own social changes and cyberspace, and nurtures Internet actors and a social environment that fit into cyber development; a state safeguards its independent Internet governance system and takes an equal part in international cooperation aimed at improving Internet governance model; a state upholds and promotes the spirit of international rule of law in cyberspace, and guards against acts of populism, isolationism and the like that hinder and undermine international rule of law in cyberspace.

The three aspects that manifest sovereignty in cyberspace are interconnected, which presents the systemic nature and integrity of activities of sovereignty in cyberspace. Respecting sovereignty in cyberspace is conducive to promoting orderly cooperation, harmony and stability in cyberspace as well as its sustainable development.

Fundamental Principles of Sovereignty in Cyberspace

I. Equality

The principle of sovereign equality set forth in the UN Charter is the primary principle that all states should follow in the exercise of sovereignty in cyberspace. All sovereign states, regardless of size, wealth, or strength, are equal before the law and have the right to participate on an equal footing in international cyberspace affairs. Each state should be treated equally, and each state is also obligated to treat others as equals.

II. Fairness

All states should uphold fairness and justice in cyberspace and facilitate a more just and equitable global Internet governance system that reflects the wishes and interests of the majority of countries, protects the legitimate rights and interests of developing countries, and ensures the people of all countries get to decide on the development of cyberspace. States should not abuse their superiority in Internet facility, technology, system and data to interfere in other countries' exercise of cyber sovereignty or promote unjust acts such as cyber hegemony or isolation.

III. Cooperation

Cyberspace is global in nature. It is difficult for any state to achieve effective governance in cyberspace solely through its own efforts. In line with the principle of cooperation in good faith advocated in the UN Charter, states should respect others as subjects of international law, follow the principle of extensive consultation, joint contribution and shared benefits, support multilateral and multi-party participation, and build a holistic governance system across multiple fields and levels to ensure the security and development of cyberspace.

IV. Peace

In interconnected cyberspace, the interests of all countries are deeply intertwined. All countries should act in conformity with the purposes and principles enshrined in the UN Charter, use the Internet for peaceful purposes, and settle cyber disputes by peaceful means. We should take effective measures to guard against the use of information and communications technology (ICT) to engage in activities that undermine peace, prevent an arms race in cyberspace, and prevent and fight cyberterrorism to maintain peace and security in cyberspace.

V. Rule of law

All states should make steady progress in domestic legislation and advance the rule of law in global governance in cyberspace, uphold the authority of international law, and oppose double standards. In the exercise of sovereignty in cyberspace domestically, states should protect the legal rights of their citizens, legal persons, and other organizations in cyberspace, and internationally, states should respect the sovereignty of others in cyberspace, and observe international law; states shall not use the Internet to interfere in the internal affairs of other countries or engage in, encourage, or support cyber activities that endanger the national security of other countries.

Sovereignty in Cyberspace in Practice

I. A number of important international documents have confirmed that the principle of national sovereignty applies to cyberspace.

The *Declaration of Principles* adopted at the World Summit on the Information Society in 2003 stated that "policy authority for

Internet-related public policy issues is the sovereign right of States". The *Tunis Agenda for the Information Society* adopted at the 2005 WSIS highlighted the key roles and responsibilities of national governments in the summit process.

In 2011 and 2015, the *International Code of Conduct for Information Security* put forward by China, Russia and other countries reaffirmed that "policy authority for Internet-related public policy issues is the sovereign right of States".

The reports of the UN Group of Governmental Experts (UN GGE) in 2013 and 2015 stressed that "state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities", and emphasized "the principle of sovereignty as the basis for increased security in the use of ICTs by States".

The Leaders Communiqué of G20 Antalya Summit in 2015 affirmed that "international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behavior in the use of ICTs".

The *Goa Declaration* at 2016 BRICS Summit reiterated that "the use and development of ICTs through international and regional cooperation and on the basis of universally accepted norms and principles of international law, including the Charter of the UN in particular political independence, territorial integrity and sovereign equality of States, the settlement of disputes by peaceful means, non-interference in internal affairs of other States as well as respect for human rights and fundamental freedoms, including the right to privacy; are of paramount importance in order to ensure a peaceful, secure and open and cooperative use of ICTs".

II. States are exercising sovereignty in cyberspace through legislative, administrative and judicial practices.

With regards to advocating and practicing principle of sovereignty in cyberspace, China stated at the 2nd World Internet Conference that respecting sovereignty in cyberspace is an important principle in the reform of the global Internet governance system. In the *Law on Cybersecurity* adopted in 2016, China embraces "safeguarding national sovereignty in cyberspace" as a fundamental purpose of cyberspace legislation. The *National Cyberspace Security Strategy* released in 2016 stresses that "national sovereignty extends to cyberspace" and upholds sovereignty in cyberspace as an important part of national sovereignty. The *Strategy on International Cooperation in Cyberspace* released in 2017 places the principle of national sovereignty on the list of the basic principles for international cooperation in cyberspace and regards "safeguarding national sovereignty and security" as the primary strategic goal of engaging in such cooperation. China has also made it clear that national sovereignty applies to cyberspace in the UN Group of Government Experts and the Open-Ended Working Group (OEWG), the Asian-African Legal Consultative Organization and in other multilateral fora.

As far as exploring the Internet development path and cyber administration models is concerned, *The Law on Cybersecurity* of Vietnam in 2018 makes it clear that "mutual respect for independence, sovereignty and territorial integrity, mutual non-interference in internal affairs, equality and mutual benefit" form the basic principles of cybersecurity cooperation. It provides a detailed list of acts that are prohibited in cyberspace such as distorting historical facts, undermining ethnic unity, offending religious belief and other acts that violate national sovereignty, interests and security. The European Union put forward "technological sovereignty" in February 2020 in a bid to reinforce its control and dominance in technologies, rules and values in cyberspace.

As for protecting domestic network from threats, disruptions, attacks and sabotage, Russia adopted the *Stable Runet Act* in May 2019 to ensure independence and reliability of its own Internet resources so that it can still function properly when it is unable to connect to servers outside the country.

In regard to protecting the rights and interests of citizens in cyberspace, the EU adopted the *General Data Protection Regulation* in May 2018 to put cross-border flow of personal data under strict control, and expands the confines of sovereignty through extra-territorial jurisdiction over processing of personal data.

Vision on Sovereignty in Cyberspace

Currently, developments in cyberspace pose grave challenges to traditional political, economic and social governance structure, while international law on cyberspace and relevant national laws and regulations are neither comprehensive nor sufficient enough to meet rising demands for governance. The introduction of principle of sovereignty in cyberspace has further defined rights and interests of various actors. It helps regulate the behaviors of governments, international organizations, private sectors, research groups, social organizations and individual citizens in cyberspace, and promote effective international cooperation on the basis of sovereign equality and mutual non-aggression, thus playing an important role in addressing all kinds of cybersecurity challenges as well as building and maintaining a sound order in cyberspace.

I. Forestall and reject cyber hegemony

Respecting sovereignty in cyberspace means countries should respect each other's own choice of development path and governance model in cyberspace and equal rights in participating in global cyberspace governance. No country should pursue cyber hegemony, interfere through leveraging Internet in other countries' internal affairs, engage in, condone or support acts that endanger other countries' national security, or undermine information infrastructure of other countries. Some countries, by putting their own national interests above those of others and the international community, have failed to honor relevant obligations set forth in the international law, imposed long-arm jurisdiction, pursued unilateralism, built trade barriers and undermined other countries' legitimate interests and sovereignty in cyberspace. The international community should work together to guard against and reject such acts and adopt corresponding sanction measures.

II. Build a more inclusive framework on global coordination and cooperation

The nature of sovereignty in cyberspace comprises mutual respect, equality, openness and inclusiveness. Advocating and practicing sovereignty in cyberspace doesn't mean that countries can act at will or adopt the beggar-thy-neighbor approach. It is natural to find diverse means of enforcing sovereignty in cyberspace, and the diversity shall exist for a long time to come. For the international community the new task at hand is how to balance sovereign rights and obligations of countries on the basis of respecting national sovereignty, with a view to sharing the benefits and dividends of digital era and maintaining peace and stability in cyberspace.

III. Define a proper scope of application for sovereignty in cyberspace

Cyberspace is an artificial space built on the foundation of information technology and characterized by multiple dimensions, wide-ranging areas and diverse actors. It breaks the traditional geographical limits and has a strong impact on the exercise of sovereignty based primarily on territorial jurisdiction and supported by personal jurisdiction. For example, as the concept and scope of cyberspace is fast expanding, there is a need to keep adapting to new circumstances in exercising sovereignty in cyberspace. Some powers are still shifting between state actors and non-state actors or institutions, leading to adjustments and adaptations. In the digital era rife with massive potential, how to effectively uphold and properly exercise sovereignty in cyberspace has become a new topical issue for the international community and requires joint efforts of all parties.

Advocating and practicing sovereignty in cyberspace does not deny the role of entities other than national governments in cyberspace governance. Nor does it dismiss the connectivity of cyberspace or free flow of information and creativity on the basis of proper order, and even less sealing off the cyberspace or breaking it up. Instead, it means facilitating a just and equitable international cyberspace order on the basis of national sovereignty and building a community with a shared future in cyberspace. States should work together under the UN framework and uphold the principles of engaging in discussions as equals, seeking common ground while shelving differences, and pursuing mutual benefits. States should strengthen communication, harmonize positions, and on the basis of upholding sovereignty in cyberspace, formulate universally acceptable international rules and codes of conduct for cyberspace. States should join efforts in consolidating broad consensus and contributing wisdom and strength, so as to build peaceful, secure, open, cooperative, and orderly cyberspace.