清华大学法学院
TSINGHUA UNIVERSITY SCHOOL OF LAW

清华大学
智能法治研究院
Institute for Studies on
Artificial Intelligence and Law
Tsinghua University

Initiative on Rule-Based International Governance of Cyberspace

Tsinghua University School of Law
Research Team

Feb.2021

Contents

Preface

Since the outbreak of COVID-19 pandemic, countries have been interdependent on each other to a unprecedented extent and mankind has shared a common weal and woe. The concept of a community of shared future for mankind, in which each has a stake, has become more and more manifest. As a global public sphere, cyberspace provides a platform for everybody to be present at the same time: opinions interact with one another; information floods instantaneously. Cyberspace involves politics, economy, culture, and technology; it engages governments, international organizations, Internet companies, technology communities, civil society, and citizens, forming an integrated, organic body. In a word, cyberspace is the online version of a community with a shared future for mankind.

As for governance, cyberspace exhibits complexity. From a technological point of view, cyberspace is layered: it can be roughly divided into the physical layer, the logical layer, and the content layer. From the perspective of governance, these strata are interrelated and interlinked. The difficulty of international governance of cyberspace lies in the disharmony between the logic of technological layering and the logic of governance connectivity.

Information technology, however, demarcated the boundaries of governance and coevolves with governance structure. In the IPv4 era, regulations on DNS resource allocation, as the core issue, is characterized by unclear governance subject, weak rules and chaotic mechanism. In the IPv6 era, technological progress has brought new opportunities and new perspectives for improving governance. International cyberspace governance requires the participation of various parties, each performing its own duties and making full use of its capabilities, and making concerted efforts to build a new system of rules.

This Initiative tries to outline a new, rule-based international cyberspace governance regime in the context of IPv6 applicatio, which looks into the future international cooperation of cyberspace governance.

Ⅰ. Tenets

The tenets of the new system of rules for international cyberspace governance is to balance freedom and order, and give consideration to both security and development.

Freedom and Order Freedom in cyberspace requires basic order. An ideal cyberspace is a public space in which all subjects of the international community freely participate and find their proper places. All parties should engage in rational consultation and orderly participation in light of their own conditions to jointly maintain the basic order of cyberspace.

Security and Development Security and development in cyberspace are mutually reinforced. A well-designed international cyberspace governance regime should give

consideration to both security and development. It should strive for security-oriented development and security-oriented security, so that all mankind can share the benefits of technology.

Ⅱ. Principles

Cardinal principles of the new system of rules for international cyberspace governance include respecting state sovereignty, protecting human rights and adapting to the patterns of technological innovation.

Respecting State Sovereignty Respecting the sovereignty of states constitutes the foundation of international community. That principle applies in cyberspace. It is necessary to understand and construe the concept of sovereignty in the context of cyberspace and in line with the underlying logic of information technology.

Protecting Human Rights Cyberspace offers crucial fora for people to speak, socialize, do business and other things. Cyberspace governance should fully safeguard individual human rights, ensuring everybody's equal opportunity to utilize cyberspace and prohibiting unreasonable and discriminatory treatment.

Adapting to Patterns of Technological Innovation The Internet is a network constructed by information technology. Patterns of technological development determines the underlying logic of cyberspace. International governance of cyberspace should adapt to the rules of code. Yet it must overcome technological instrumentalism and technocratism so as to subject technology to ethical control.

Ⅲ. Goals

The goals of good, effective governance depends upon what problems it solve and what visions it should achieve.

The problems lies ahead are as follows:

i. Who Uses What Rules to Govern Cyberspace

In terms of cyberspace governance at the global level, objects are complex, subjects multiple, methods diverse, and interests wide-ranged. Based on the principle of extensive participation, the new system of rules should clarify the governing subjects and corresponding rights and responsibilities, and define grounding norms as well as their conditions of application.

ii. Cybersecurity Regulation: Sovereignty v. Human Rights

The lack of unified international rules in the field of cybersecurity regulation partly results from a big ideational debate: the antinomy between "sovereignty and human rights". Generally speaking, developed countries apply human-rights based approaches to cyber security laws and policies. On the other side, developing countries are deeply concerned with sovereignty and security and push for tightened regulation accordingly.

iii. Bridging The Global Digital Divide: Domestic v. International

Obviously, information and communication technology (ICT) is closely related to a country's comprehensive power; digital economy has become a wrestling field of global competition. Because of disparate technological and economic power among nations, the global digital divide is deepening day by day. The uneven development of digital economy and the unequal voice of network governance have become the "East African Rift Valley" that has torn apart global justice. It become the reverse tension for the community of shared future of mankind to move forward together.

In terms of governance structure, a paradox looms. Efforts to bridge the digital divide within a country may enlarge the information gap in the international arena. As the digital economy industry is both capital-intensive and technology-intensive, measures taken by developed countries to eliminate the domestic digital divide objectively aggravate the shortage of capital and technology in developing countries.

The visions the new rules should achieve are the following:

i. Broad and Balanced Participation

As for the cyberspace global governance, the interests of all nations and the development of the whole mankind are at stake. This vision requires to guarantee all parties the right to participate. To establish a multi-stakeholder governance structure where all parties perform their respective duties, the new rule system strives to forge a unified system with balanced power and responsibility, verified by an open and transparent decision-making procedure, and guided by intelligible governance norms with clear applicable conditions.

ii. Security by Sovereignty

The protection of human rights cannot be realized without the upholding of sovereignty. For global security governance, this vision is to seek the greatest common ground among all countries, premising full respect for different interpretations of national security. Thus, the new system of rules calls for equality and mutual respect among global governing subjects; Meanwhile, it should give full consideration to the unbalanced status quo of economic development, globe-wide and region-wide, so as to formulate security norms featuring fairness and justness.

iii. For Common Future

No subject is immune from the future of shared community of humankind. A thriving forest has its small trees, a burned down forest has no trees. To usher a bright future, global parties are required to step up coordination, put aside disputes and forge ahead hand in hand. To circumnavigate the "tragedy of the Commons" and the "anti-tragedy of the Commons", the digital economy must be guided by a new rule system that, by transforming the non-cooperative game into a cooperative one, advances the well-being for all.

Ⅳ. Our Initiative

i. Subjects

On the front of UN, global governing subjects should build on the wide participation provided by the UN multi-stakeholder platform, accelerate the construction of a governance model featuring the lead by sovereign states and joint participate of various players. On the front of ICANN, efforts are needed to facilitate the transformation and upgrading of decision-making process and governance model, into a structure of differential order in which each player assumes proper rights and responsibilities.

The differential structure we propose is as follows:

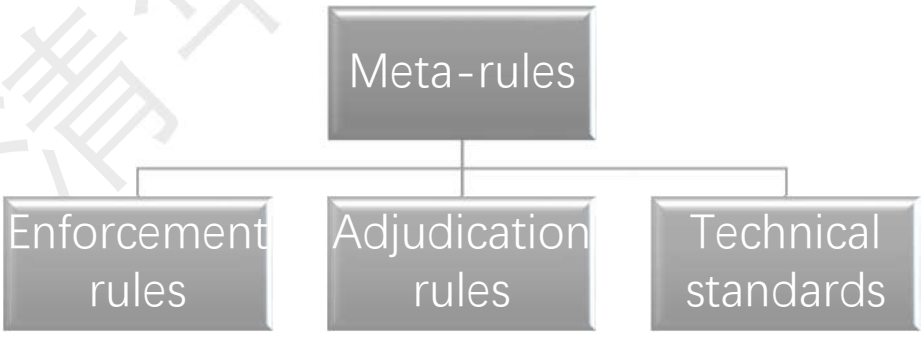
Governments and IGO: Subject of Meta-rules making & international internet dispute adjudication.

International technical organization: Subject of technical standard formulation

Citizens & Multinational Internet Enterprises: Subject of opinions.

ii. Norms

For existing norms that are scalable, transparent and equitable, we should accelerate the revision process, expand participation, adapt governance content, and clarify the scope of application. For regulatory vacuums where no acknowledged norm currently exists, we should expedite the formulation of new norms with the UN as the main platform. Finally, we hope to form a double-layered and three-aspect standard system, encompassing the framework of meta-rules, enforcement rules, adjudication rules and technical standards.



iii. Security

In regard to cybercrime, the international community should employ a stepwise strategy to strengthen the regulation of traditional crime. The first step is to construct a cooperative framework. Relying on the United Nations platform, an intergovernmental

supervision and enforcement agency for cybercrime shall be established. The new agency would be expected to strengthen cooperation between Governments and Interpol, while amplifying Interpol's capabilities in information collecting and law enforcement coordinating. The second step is to formulate a set of governance norm. The cybercrime governance norm shall be embedded in the UN framework and grounded on consensus. Led by the Open-Ended Working Group (OEWG), the drafting of new norms should specify the nature and extent, constitutive elements and legal consequences of cybercrime; guide by of the Group of Governmental Experts (GGE), the draft should also clarify the scope and applicable conditions of existing international rules.

In regard to cyber terrorism, the international community should think globally and act globally. Parties need to temporarily shelve disputes on politics, culture or religion, size up the situation, and expand the cybercrime regulation to address prominent issues that endanger global security and development. Looking into future, they should conceive the establishment of a global anti-terrorism agency resting on the UN framework.

As for regulation on cross-border data flows, it should be oversight by a classified supervision system. To achieve the goal, the international community need to reach consensus on the following two grounds. First, the consensus on data classification. A scientific and equitable data classification catalogue should be established to reflects concern for the inequality in international socio-economic and technological development. Second, the consensus of regulatory methods. A international "regulatory toolbox" for cross-border data flows should be built based on full investigation and discussion by all peer countries on current data regulatory methods. Grounded on the consensuses, governments can develop their own integrated data regulation approach in accordance with their own domestic policies.

For DNS management, we put forward three proposals, in respective of technological development, strategic deployment and governance subject. First, it is necessary to steadily promote research on security technology and actively explore DNS security solutions other than Domain Name System Security Extensions (DNSSEC). Second, we should guard against the potential regional divide brought by DNSSEC global deployment. ICANN, the governing subject of DNSSEC, should pay sufficient attention to the voices of Regional Internet Registries (RIR) in its multi-stakeholder decision-making of deployment strategy, thereby incorporating interests of different regions. Third, it's pertinent to increase the impact of governmental representatives in ICAAN. Internally, ICAAN Board should entrust the decision power to the Governmental Advisory Committee (GAC). Externally, the International Telecommunication Union (ITU) should proactively weigh in on the global DNS governance through Empowered Community in ICANN.

iv. Development

The international digital divide takes form in three layers. As such, the governance of each layer diverges on missions. First, for bridging the gap of information

accessibility and communication network connectivity among countries, the mission focus is to set up new infrastructure management departments. Second, for bridging the using gap caused by disparity in ICT literacy, the core of governance is to foster a favorable using environment, and to create skill training departments and data management departments. Third, for bridging the knowledge/capacity gap and reduce the consequential unbalance in magnitude of social influence delivered via ICT, the key to governance lies in the establishment of integration management departments.

In order to bridge the digital divide, we propose to set up supporting institutions under the framework of "One Belt and One Road" to form a cooperation mechanism.

Institutions

The cornerstone to bridging the first digital divide is the new infrastructure management sector (NIMS), which is the focus of China-foreign cooperation today, and would also become the focus of global digital divide governance in the future.

The skills training department and the data management department are committed to creating a favorable network-using environment. They are also devoted to building comprehensive laws and regulations to reduce the second digital divide on all fronts.

Integration management department encompasses digital economy development department and information content management department. The former shall manage e-commerce and specific trade projects, and the latter shall coordinate countries in resolving cyberspace contradictions at the content level, which may arise from religious, political and cultural collisions , or from underlying ideological incongruity.

A cooperation mechanism

We will advance the development of the "Digital Silk Road", cooperation mechanisms, governance rules and technical standards. First of all, continue to promote the diversification of cooperating subjects, and appeal technologically advanced enterprises to take part in international cooperation programs under One Belt and One Road. Second, we should encourage multilateral regional cooperation within One Belt and One Road framework, and pursue intergovernmental treaties. Third, we will vigorously encourage scientific and technological innovation and support the introduction of new technological standards. Finally, we should strengthen technical personnel training and exchanges, carry out specialized training programs, and support study-abroad programs, and aid countries along the Belt and Road by improving their technological capacities and promoting cultural exchanges.