“一带一路”国家网络空间区域治理规则框架草案（学者建议稿）

Regional Framework Rules of Cyberspace Governance in OBOR Countries (Scholars’Proposal)

面向 IPv6 的网络空间国际治理联合研发与示范项目课题组（2023 年 5 月）
Joint R&D and Demonstration Project on International Governance of Cyberspace for IPv6 Team, May 2023

目　　录

第一章　总　　则

Chapter I General Principles

第一条 【宗旨】为维护网络空间内的国家主权，促进人权保障，增强国际互联网的安全可信和综合治理能力，推动网络信息技术、产业、应用的创新和变革，促进“一带一路”国家（以下简称“各国”）网络空间区域治理的共享合作与各国互联网的高质量发展，提高数据资源有序开放共享和信息安全保护水准，根据《联合国宪章》的基本精神和现行国际法基本原则，制定本规则。

Article 1. PURPOSE. In accordance with the basic spirit of the Charter of the United Nations and the fundamental principles of international law, the following rules are formulated so as to safeguard state sovereignty and promote human rights protection in cyberspace, improve the security and credibility of the global Internet and capacities of comprehensive governance, encourage innovation and change in network information technology, industry and applications, and promote, encourage regional governance in cyberspace sharing and cooperation among OBOR countries (hereinafter referred to as "countries") as well as high-quality Internet development in each country, and to strengthen the orderly open sharing of data resources and the level of information security protection.

第二条 【基本指引与根本目标】网络空间区域治理应以主权平等、和平合作、公平正义、开放包容、互利共赢的价值理念为基本指引，以打造政治互信、经济融合、文化包容的命运共同体、利益共同体和责任共同体为根本目标，着力构建良好秩序，共享全球发展成果。

Article 2. FUNDAMENTAL PRINCIPLES AND OBJECTIVES. Regional cyberspace governance should follow principles of sovereign equality, peace and cooperation, fairness and justice, openness and inclusiveness, mutual benefit and progress; and should aim to create a community of common destiny, interests and responsibilities based on mutual political trust, economic integration, and cultural integration, and endeavor to construct a well order in which mankind shares the achievements of global development.

第三条 【尊重主权原则】网络空间区域治理应当尊重各国主权。网络空间国家主权独立、平等。管辖权与防卫权是一国主权的体现，应得到各国尊重与维护。各国应遵守国际法基本原则和一般规则，不得通过互联网侵犯他国主权、干涉他国内政，并对主权控制范围内的网络活动负有审慎预防和安全保障之义务。

Article 3.RESPECT SOVEREIGNTY. Regional governance in cyberspace should respect the sovereignty of all countries. State sovereignty in cyberspace is independent and equal. Rights of jurisdiction and defense are the embodiments of a country's sovereignty and should be respected and maintained by all countries. Countries must obey the fundamental principles and general rules of international law, refrain from infringing on the sovereignty of other countries through the Internet and interfering in the internal affairs of other countries, and bear the responsibility for prudent prevention and security of cyber activities within the scope of sovereign control.

第四条 【人权保障原则】网络空间区域治理应充分保障人权。各国应保护个人信息与隐私安全，合作打击网络攻击、网络犯罪与网络恐怖主义。各国应保障互联网平等接入和顺畅交流，禁止歧视和一切不合理的差别对待，共同

推动互联网基础设施建设，保障数据安全流动，努力缩小数字鸿沟，维护和促进最广大范围内的互联网发展权益。

Article 4.HUMAN RIGHTS PROTECTION. Regional governance in cyberspace should fully protect human rights. Countries should protect the security of personal information and privacy, and cooperate to combat cyber attacks, cybercrimes and cyber terrorism. They should guarantee equal access and smooth communication in the Internet, prohibit discrimination and other unreasonable differential treatments. They should jointly promote the development of Internet infrastructure, ensure the safe flow of data, aim to close the digital divide, and protect and promote the rights and interests of the broadest range of Internet development.

第五条 【法治与公正原则】网络空间中的一切活动和行为必须依法进行，不得违反国际法规则、原则和基本精神。各国不应滥用自身在网络领域的设施、技术、系统、数据等方面的优势地位，对他国行使网络主权进行干涉，或推行网络霸权、网络孤立等不公正行为。

Article 5. RULE OF LAW AND JUSTICE. All activities and acts in cyberspace must comply with the law and must not contravene the regulations, principles, and basic spirit of international law. Governments should not use their dominating position in the cyber domain in terms of facilities, technology, systems, and data to interfere with other countries' exercise of cyber sovereignty and to pursue cyber hegemony, cyber isolation, and other unfair activities.

第六条 【善意合作原则】各国在网络空间区域治理中应当求同存异、相互尊重，坚持共商共建共享的理念，共同推进发展、共同维护安全、共同参与治理、共同分享成果，在促进区域互联网发展的同时，共同为全球的网络空间治理作出积极贡献。

Article 6.GOODWILL AND COOPERATION. Countries should seek common ground and respect one another in regional cyberspace governance, adhere to the ideas of extensive consultation, joint contribution and shared benefits, jointly promote development, maintain security, participate in governance and share results, so as to make positive contributions to global cyberspace governance while promoting regional Internet development.

第七条 【克制礼让和对等原则】各国行使网络主权，应本着克制、礼让和对等的精神，减少摩擦和对抗，避免相互掣肘，促进经济合作与安全协作。

Article 7.COMITY AND RECIPROCITY. Countries exercising cyber sovereignty should follow the principles of self-restraint, comity and reciprocity, so as to reduce friction and confrontation, avoid mutual constraints, and promote economic cooperation and security collaboration.

第八条 【柔性治理原则】各国应增强互信，积极合作，全面提升互联网治理能力和水平，合作建立基于信用的柔性治理体系，实现守信激励和失信约束，打造安全善意诚信的网络空间。

Article 8 FLEXIBLE GOVERNANCE. Countries should strengthen mutual trust, actively collaborate, comprehensively improve Internet governance capacity, cooperate to establish a credit-based flexible governance system, achieve incentives for trustworthiness and constraints for breach of trust, and establish a secure, good faith, and honest cyberspace.

第九条 【能力提升原则】各国应积极对话，推动多领域、多层次、多方面的合作，提升区域整体安全水平和防御能力，促进区域经济和社会发展。

Article 9. CAPACITY ENHANCEMENT. Governments should actively engage in dialogues and encourage multi-field, multi-level, and multi-faceted cooperation to improve the region's overall security and defense capability, as well as to promote regional socio-economic development.

第二章 网络空间发展

Chapter II Cyberspace Development

第十条 【支持合作开发】鼓励各国在信息网络技术、产品、服务创新和人才培养等领域进行深度合作，协作攻克威胁网络安全的技术难题，共同开发区域网络安全产品，创新网络经济发展模式，打造高水平高素质的网络人才队伍。

鼓励合作开发网络安全预警平台，建立区域共享的安全预警机制，弥补网络管理能力的不均衡。

支持研究开发普惠医疗、普惠教育和有利于未成年人健康成长的网络产品和服务。

Article 10. COOPERATIVE DEVELOPMENT. Countries shall intensify their cooperation in the fields of information network technology, product and service innovation, and talent training, as well as to collaborate to overcome technical problems that threaten cybersecurity, develop regional cybersecurity products collaboratively, innovate network economic development models, and build a high-level, high-quality network talent team.

Countries shall encourage collaboration in developing a network security alerting platform and the establishment of a regional shared security alerting mechanism to compensate for disparities in network management capacities.

Countries shall enhance research and development of inclusive health care, inclusive education, and inclusive network products and services that promote minors' healthy development.

第十一条 【畅通交流渠道】鼓励多领域、多层次、多方面的区域间交流合作。支持各国的行业组织、企业、教育和科研机构、有关专业机构和人员等开展区域间网络数据安全技术开发利用的交流共享活动，促进网络安全的教育和培训。

Article 11 INTERNATIONAL COMMUNICATION CHANNEL. Countries shall endorse inter-regional, multi-field, multi-level, and multi-faceted exchanges and collaboration, support trade organizations, enterprises, educational and scientific research institutions, relevant professional institutions and personnel of various countries to carry out inter-regional exchanges and sharing activities on the development and utilization of network data security technologies, and promote education and training on cybersecurity.

第十二条 【保障多方参与】各国应当积极推动形成政府、企业、相关社会组织、公众共同参与治理的良好环境，推动与其他国家、地区、国际组织在网络安全、网络数据处理等领域的规则、标准等的互认。

Article 12 ENSURE MULTI-PARTICIPATION. Countries should actively promote the formation of a well environment for governments, enterprises, relevant social organizations, and the public to participate in governance, and promote mutual recognition of cybersecurity and data processing rules and standards made by other countries, regions, and international organizations.

第十三条 【促进数据安全有序流动】在保障数据安全和保护个人信息、隐私权益的前提下，推动区域间数据安全有序流动，共同挖掘数据经济新增长，促进网络信息技术的创新发展，助力“一带一路”区域间跨境要素流动规则和风险防范机制的建立。

Article 13. PROMOTE SAFE AND ORDERLY DATA FLOW. On the premise of ensuring data security and protecting personal information , privacy rights and interests, countries shall promote the safe and orderly flow of data among regions, jointly explore the new growth of data economy, promote the innovation and development of network information technology, and facilitate the establishment of cross-border factor flow rules and risk prevention mechanisms between regions under the Belt and Road Initiative.

第十四条 【尊重技术发展规律】网络空间区域治理应尊重和适应技术发展的客观规律，促进人与技术共生共进。

尊重网络空间互联互通的特性，维护互联网的统一，避免互联网“碎片化”。各

国不得恶意排斥他国的供应商、信息技术和产品、光纤电缆等设施，也不应凭借自身技术、经济或政治的优势，不公平分配或封锁重要网络资源，危害全球和区域供应链安全。

各国应当着力克服互联网协议第四版（IPv4）所面临的网络地址消耗殆尽、服务质量难以保证以及跨国协同治理低效等问题，充分发挥互联网协议第六版（IPv6）在网络地址、创新空间和区域治理上的优势，提升本国互联网的承载能力和服务水平。

掌握技术优势的国家可向需要帮助的国家提供必要援助。

Article 14. RESPECTING PATTERNS OF TECHNOLOGICAL DEVELOPMENT. Regional governance in cyberspace should respect and adapt to the objective patterns of technological development, and promote the coexistence and progress of mankind and technology.

Countries should respect the nature of connectivity in cyberspace, maintain the unity of the Internet and avoid fragmentation of the Internet. Countries should not maliciously exclude other countries' suppliers, information technology and products, fiber optic cables and other facilities, nor should they take advantage of their own technological, economic, or political advantages to unfairly distribute or block important cyber resources and jeopardize the security of global and regional supply chains.

Countries should strive to overcome the problems of Internet Protocol Version 4 (IPv4), such as the depletion of network addresses, the difficulty of ensuring service quality, and the inefficiency of transnational collaborative governance, and give full play to the advantages of Internet Protocol Version 6 (IPv6) in network addresses, innovation space and regional governance, so as to improve the carrying capacity and service level of their own network.

Countries with technological advantages may provide necessary assistance to countries in need.

第三章　网络空间安全

Chapter III Cyberspace Security

第十五条 【保护网络基础设施】各国得依照国内法规定保护网络基础设施。任何国家、军队、政府以及政府授权的组织和个人皆不得对网络基础设施进行攻击或损害。

一国攻击另外一国的网络基础设施的行为将侵犯该国的主权。一国得根据主权原则限制或保护互联网接入。接入国际互联网不意味着该国放弃其主权。

对于一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、公共利益的关键信息基础设施，可实行重点保护和防御，必要时可请求他国予以协助。

Article 15. NETWORK INFRASTRUCTURE PROTECTION. Countries have the right to protect their network infrastructure in accordance with domestic laws. No country, military, government, government-authorized organizations or individuals shall attack or damage network infrastructure of other countries.

An attack on another country's network infrastructure constitutes a violation of that country's sovereignty.

A state may restrict or protect Internet access in accordance with the principle of sovereignty. Access to the Internet does not mean that the country gives up its sovereignty.

In case of damage, loss of function or data leakage, key information infrastructure that may seriously endanger national security and public interests, a country may carry out critical measures of protection and defense, and may request assistance from other countries when necessary.

第十六条 【互联网名称和数字地址安全】互联网根服务器、通信协议和 IP 地址等互联网关键资源是全球公共资源。各国应积极促进互联网关键资源的公平分配和管理，积极推动互联网名称和数字地址分配机构的国际化改革，切实提高其代表性和决策、运行的公开透明。

Article 16. SECURITY OF INTERNET NAMES AND DIGITAL ADDRESS. Internet root servers, communication protocols and IP addresses and other key Internet resources are global public resources. Countries should actively promote the fair allocation and management of Internet key resources and the international reform of the Internet name and digital address allocation authority, and effectively improve its representativeness and the openness and transparency of its decision-making and operation.

第十七条 【禁止网络窃听】禁止国家间进行网络窃听、监听活动。为保障各国互联网的安全运行，主权国家应享有管理其网络的权利，有权对未经授权的网站设置接入许可、对不服从管理的网站停止提供服务等。

Article 17. PROHIBITION OF NETWORK EAVESDROPPING. Network eavesdropping and wiretapping activities are prohibited among countries. To ensure the safe operation of the Internet in each country, countries have the right to regulate their networks, impose access licenses for unlawful websites, and discontinue providing services to websites that do not conform to management, etc.

第十八条 【禁止网络攻击和网络战争】禁止发动网络攻击和网络战争。应首先寻求磋商、谈判等和平方式友好解决冲突，必要时可请求本规则设置的相关机构和组织进行协调，以最小代价解决争端。

Article 18. PROHIBITION OF CYBER ATTACKS AND WAR. Launching of cyber attacks and cyber war are prohibited. Consultations, discussions, and other peaceful methods of resolving disputes shall be sought first, and if necessary, relevant agencies and organizations established by these rules may be requested to collaborate in order to resolve disputes at the minimum cost.

第十九条 【未成年人保护】各国应依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。合作打击利用网络进行的儿童色情和暴力犯罪。

网络数据处理者处理不满十四周岁未成年人的个人信息或其他网络数据的，应当取得未成年人父母或者其他监护人的同意。各国国内法有规定的，从其规定。

各国网络空间治理主体得依国内法，自觉承担对危害或者可能危害未成年人身心健康发展之内容的审查、筛选和拦截等义务，依法惩处有害信息的制造、传播和提供者。有条件的还应向本国和他国的个人、组织提供非法内容的举报渠道。

Article 19. TEENAGERS PROTECTION OF TEENAGERS. Countries should punish according to law the use of the Internet to engage in activities that endanger the physical and mental health of minors, and provide a safe and healthy Internet environment for minors. They should cooperate to combat Internet use of child pornography and violent crime.

Where an online data processor processes the personal information or other online data of a minor under the age of 14, it shall obtain the consent of the minor’s parents or other guardians. Where there are provisions in the domestic laws of each country, such provisions shall prevail.

Cyberspace governance bodies of all countries may, in accordance with domestic laws, consciously undertake the obligation to review, screen and intercept content that harms or may harm the physical and mental development of minors, and punish the production, dissemination and provider of harmful information according to law. If conditions permit, channels for reporting illegal content should also be provided to individuals and organizations in their own countries and other countries.

第二十条 【电子证据调取跨境协作】对于发生在一国境内的网络犯罪，或针对该国进行的网络犯罪，该国执法部门请求他国公权力机关、企业或个人提供相关电子证据进行协助的，他国可依国内法的规定，在不损害本国的国家安全、公共利益和个人重大合法权益的前提下提供必要协助。

Article 20. CROSS-BORDER COLLABORATION OF ELECTRONIC EVIDENCE RETRIEVAL. For cybercrimes committed within the territory of a country or against that country, if the law enforcement authorities of that country request the public authorities, enterprises or individuals of another country to provide relevant electronic evidence for assistance, the country requested may, in accordance with the provisions of its domestic law, provide necessary assistance on the premise of not harming its national security, public interests and significant rights and interests of individuals.

第二十一条 【保护数据安全】对于承载一国经济、文化、国防安全等重大公共利益和公民权益的数据，应在保护数据安全的前提下开展处理活动。

开展数据处理活动，应当遵守国际条约、习惯和国际法原则，不得损害他国的国家安全、公共利益与公民的合法权益。

各国应督促国内数据处理者在网络数据处理活动中，自觉承担国际和国内社会责任，尊重社会公德、商业道德和职业道德，履行相应的数据安全保护义务。

Article 21. PROTECTION OF DATA SECURITY. Data conveying a country's economy, culture, national defense security, and other key public interests, as well as citizens' rights and interests, should be processed under the premise of data security.

Data processing activities should adhere to international treaties, norms, and legal principles, and shall not jeopardize national security, public interest, or the legitimate rights and interests of citizens of other nations.

Countries should urge domestic data processors to consciously assume international and domestic social responsibilities, respect social justice, business ethics and professional ethics, and fulfill the corresponding data security protection obligations in their network data processing activities.

第二十二条 【保护个人信息与隐私】各国在商业合作、司法协作或其他过程中确有必要收集他国公民个人信息的，应当基于明确、合理的目的，遵循合法、正当、必要和诚信的原则，在取得相关主体同意的基础上针对个人信息的收集、存储、使用、加工、传输、提供、公开、删除等各个环节妥善履行保护义务。被收集国有相关规定，得依该国规定进行。

Article 22. PROTECTION OF PERSONAL INFORMATION AND PRIVACY. If it is truly necessary for states to collect personal information of citizens of other countries in the course of commercial cooperation, judicial cooperation or other processes, they shall do so for clear and reasonable purposes and in accordance with the principles of legality, legitimacy, necessity and good faith. On the basis of obtaining the consent of the relevant subject, the obligation of protection shall be properly fulfilled in respect of the collection, storage, use, processing, transmission, provision, disclosure, deletion and other links of personal information. If the country where the data is collected has relevant regulations, such regulations shall be complied with.

第二十三条 【合作打击网络犯罪和网络恐怖主义】探索建立更具包容性和透明度的新网络犯罪公约。面向人工智能、云计算等新技术带来的新威胁，瞄准复杂多样的网络犯罪新形态和网络恐怖主义新威胁，探索建立覆盖所有缔约方合理诉求和重点关切、程序透明和机制合理的新公约。

Article 23. COOPERATION IN COMBATING CYBERCRIME AND CYBERTERRORISM. Countries shall explore to establish a new cybercrime convention that is more inclusive and transparent. To address the new threats posed by new technologies such as artificial intelligence and cloud computing, and to take aim at new forms of complex and diverse cybercrimes and new threats of cyber terrorism, countries shall explore to establish a new convention that covers the legitimate appeals and major concerns of all Contracting parties, with transparent procedures and reasonable mechanisms.

第四章　网络治理执行机制信用体系

Chapter IV Credit System for Network Governance Enforcement Mechanism

第二十四条 【网络信用体系建设】合作建立网络空间信用体系，全面提升区域网络信用信息管理能力，推动区域信用状况认定标准统一，实现基于信用的事前风险防范和安全预警，打造安全可信的“一带一路”网络空间，为区域经济发展和信息交流提供保障。

Article 24 NETWORK CREDIT SYSTEM CONSTRUCTION. Countries should cooperate in establishing a credit system in cyberspace, comprehensively improve the regional network credit information management capabilities, promote the unification of regional credit status determination standards, realize credit-based prior risk prevention and security warning mechanism, create a safe and reliable ORORcyberspace for regional economic development and provide guarantee for regional economic development and information exchange.

第二十五条 【信用状况认定】各国应根据合法、客观、谨慎、关联的原则，对照网络信用信息目录和网络信用状况认定标准，对信用主体的信用状况进行认

定并载入信用档案。

网络信用信息目录旨在规范信用信息纳入范围。信用信息采集不得超出网络信用信息目录规定的范围。

网络信用状况认定标准旨在规范信用状况认定和信用档案记载的原则、依据、和评级标准。网络信用状况认定和信用档案记载须严格遵照网络信用状况认定标准进行。

网络信用信息目录和网络信用状况认定标准由各国协商确定。各国可依国内法规，编制适用于本国的网络信用信息补充目录和网络信用状况认定标准细则。

Article 25. CREDIT STATUS DETERMINATION. Countries shall, in accordance with the principles of legality, objectivity, prudence and relevance, identify the credit status of the credit subject and load it into the credit file according to the network credit information directory and network credit status identification criteria.

The network credit information directory aims to standardize the credit information included in the scope. The collection of credit information shall not exceed the scope stipulated in the catalogue of network credit information.

The standard of network credit status identification aims at standardizing the principle, basis and rating standard of credit status identification and credit file recording. The identification of network credit status and the recording of credit files shall strictly comply with the identification standards of network credit status.

The catalogue of network credit information and the standards for the identification of network credit status shall be determined by the countries through consultation. Each country may, in accordance with its domestic laws and regulations, compile supplementary catalogues of online credit information and detailed rules on standards for the identification of online credit status applicable to its own country.

第二十六条 【信用信息管理】各国应以统一或相互可识别的标识建立信用主体信用档案，并向本规则内成员国家开放查询入口。

鼓励信用档案和其他信用信息的区域共享。

信用信息共享应遵循尊重各国主权、保护基本人权的原则，不得危害国家安全，不得侵犯个人信息和隐私权益。

Article 26. CREDIT INFORMATION MANAGEMENT. Countries shall establish credit files of credit subjects with a uniform or mutually identifiable logo and open the

inquiry portal to member countries within rules stipulated in this Regional Framework Rules.

Regional sharing of credit files and other credit information is encouraged.

Credit exchange of information shall respect each country's sovereignty and protect basic human rights, not to jeopardize national security or to breach personal rights to information or privacy.

第二十七条 【区域信用预警平台】各国协同建立统一的区域信用预警平台。对于本国内有严重失信行为的信用主体，各国应主动在信用预警平台进行风险预警；各国发现他国信用主体有严重失信行为的，应将相关信息提交区域信用预警协调机构，由区域信用预警协调机构决定发布预警信息。

Article 27. REGIONAL CREDIT ALERT PLATFORM. Countries shall jointly establish a unified regional credit early alert platform. Countries should take the initiative to conduct early risk alert on that platform for the credit subjects with serious trust-breaking behaviors in their own countries. If a country finds that a credit subject of another country has committed serious dishonesty, it shall submit the relevant information to the regional credit early warning coordinating body, which shall decide to issue the early alert information.

第二十八条 【守信激励和失信约束】对于信用状况良好的信用主体，各国可依照国内法给予激励。对于失信的信用主体，各国可以依照国内法实施信用惩戒。信用主体受到守信激励和失信惩戒应记入信用档案。

各国可对他国严重失信的信用主体实施失信约束，约束措施应由各国协商一致确定。约束措施不应违背《联合国宪章》和国际法基本原则。

Article 28. CREDITWORTHY INCENTIVES AND DISCIPLINE. Countries may give incentives to credit subjects with good credit standing in accordance with their domestic laws. Countries may, in accordance with their domestic laws, impose credit punishments on credit subjects that break faith. The subject of credit who receives incentives to keep faith and punishments for breaking faith shall be recorded in credit files.

Countries may impose restrictions on other countries' seriously dishonest credit subjects, and the restrictive measures shall be determined by consensus of all countries through consultation. Binding measures should not violate the Charter of the United Nations and the basic principles of international law.

第二十九条 【信用修复】信用信息记录有误的应予以更正。各国应制定信用修复规则，采取信用修复措施，为信用主体提供投诉、反馈等救济途径。

区域信用预警平台上的信用信息有误的，由区域信用预警协调机构负责更正。救济措施和更正标准，由区域信用预警协调机构制定。

Article 29. CREDIT REPAIRMENT. Credit information recorded in error should be corrected. Countries should make credit repair legislations, implement credit repair procedures, and provide credit subjects with feedback, complaints, and other forms of relief.

If the credit information on the regional credit alert platform is erroneous, it is the responsibility of the regional credit warning coordinating agency to fix it. The regional credit alert coordination body shall establish remedies and corrective standards.

第五章　网络治理区域合作运行机制

Chapter V Operational Mechanisms for Regional Cooperation in Network Governance

第三十条 【规则制定】在尊重网络主权和平等协商的基础上，积极制定具有包容性、可行性和发展性的区域网络空间治理规则。

各国应在本框架规则的指引下，积极制定区域网络空间安全规则、数字经济合作规则、信用信息评价与共享规则、区域网络空间争端磋商与调停规则等。

Article 30. RULEMAKING. Countries should actively formulate rules for regional cyberspace governance that are inclusive, feasible and developable on the basis of respecting cyber sovereignty and consultations on an equal footing.

Under the guidance of this Framework Rules, countries should actively formulate rules on regional cyberspace security, rules on digital economy cooperation, rules on credit information evaluation and sharing, and rules on consultation and mediation of regional cyberspace disputes.

第三十一条 【合作平台】合作建立网络安全预警平台和区域信用预警平台，探索建立区域数字经济合作平台和区域网络空间技术研发与交流平台。

Article 31. COOPERATION PLATFORM. Countries should cooperate in establishing a network security alert platform and regional credit alert platform and explore for a regional digital economy cooperation platform and a regional cyberspace technology R&D and exchange platform.

第三十二条 【设立网络安全预警机构】在尊重各国主权的基础上，依照平等、公正、民主、开放、科学的原则设立网络安全预警机构。

设立咨询委员会，为预警机构的决策提供咨询意见。咨询委员会的成员由科学

技术机构、商业机构、其他组织和相关专家组成。

设立决策委员会，以咨询意见为基础，行使最终决策权。决策委员会的成员由各国政府组成。

Article 32. ESTABLISHING AN CYBERSECURITY ALERT INSTITUTION. Countries should establish a cybersecurity early warning institutions on the basis of respect for national sovereignty, in accordance with the principles of equality, justice, democracy, openness and scientificity.

An advisory committee to provide assistance to alert institutions on decision-making shall be established. Members of that committee shall comprise of Scientific and technological institutes, commercial institutions, other organizations, and relevant experts.

A decision-making committee to exercise final decision-making authority based on advisory opinions shall be established. The members of that committee shall be composed of governments from all countries.

第三十三条 【设立区域信用预警机构】在尊重各国主权的基础上，依照平等、公正、民主、开放、科学的原则设立区域信用预警机构。

设立咨询委员会，为预警机构的决策提供咨询意见。咨询委员会的成员由科学技术机构、商业机构、其他组织和自然人组成。

设立决策委员会，以咨询意见为基础，行使最终决策权。决策委员会的成员由各国政府组成。

Article 33. ESTABLISHING REGIONAL CREDIT ALERT AGENCIES. Countries should establish a regional credit alert agencies on the basis of respecting national sovereignty, in accordance with the principles of equality, justice, democracy, openness and scientificity.

An advisory committee to provide assistance to alert institutions on decision-making shall be established. Members of that committee shall comprise of Scientific and technological institutes, commercial institutions, other organizations, and relevant experts.

A decision-making committee to exercise final decision-making authority based on advisory opinions shall be established. The members of that committee shall be composed of governments from all countries.

第三十四条 【经费保障】本规则框架下规范性文件制定、平台建立和机构设立等活动所需经费，由各国按公平原则协商筹备。

经费份额可依各国经济发展水平等实际情况进行合理调整。

Article 34. FUNDING. The funds required for activities such as the formulation of normative documents, the establishment of platforms and the establishment of institutions under this Framework Rules shall be prepared by all countries through consultation in accordance with the principle of equity.

The share of funds may be reasonably adjusted according to the actual situation such as the level of economic development of each country.

第六章　附　　则

Chapter VI Definitions

第三十五条 【数据】本规则所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力

网络数据的处理，包括网络数据的收集、存储、使用、加工、传输、提供、公开等。

Article 35. DATA. The “Data” in this Framework Rules refers to any electronic or other means of information on the record.

“Data Processing” means the collection, storage, use, processing, transmission, provision, and disclosure of data.

“Data Security” entails taking the required steps to ensure that data is effectively protected and used lawfully, as well as having the ability to guarantee a continual state of security.

“Network Data Processing” means the collection, storage, use, processing, transmission, provision, and disclosure of network data.

第三十六条 【个人信息】本规则所保护的网络空间中的个人信息，是指主要以电子方式记录的与已识别或者可识别的自然人有关的各种信息，不限于利用网络产生或在其中处理的个人信息，但不包括匿名化处理后的信息。

Article 36. PERSONAL INFORMATION. “Personal information” in cyberspace protected in this Framework Rules refers to a variety of information related to identified or identifiable natural persons recorded mainly in electronic form, not limited to the use

of the network generated or processed in the personal information, but does not include the anonymization of the information after processing.

第三十七条 【网络信用与网络信用信息】本规则所称网络信用，是指某一 IP 地址（下称信用主体），在网络空间活动中遵守法定义务、履行约定义务的状态。

本规则所称网络信用信息，是指可用于识别、分析、判断信用主体信用状况的客观数据和资料。

Article 37.NETWORK CREDIT AND NETWORK CREDIT INFORMATION.“Network Credit” in this Framework Rules refers to an IP address (hereinafter referred to as the credit subject), in the cyberspace activities to comply with the legal obligations, the state of fulfilling the agreed obligations.

“Network Credit Information” refers to the objective data and information that can be used to identify, analyze and judge the credit status of the credit subject.