Federal State Budgetary Educational Institution
institution of higher education
**"RUSSIAN ACADEMY OF NATIONAL ECONOMY
AND CIVIL SERVICE
UNDER THE PRESIDENT OF THE RUSSIAN FEDERATION"**

North-West Institute of Management

On the rights of the manuscript

Alexeyev George Valerievich

LEGAL INTERACTION OF INTERNATIONAL NON-GOVERNMENTAL ORGANIZATIONS AND STATES IN CYBERSPACE

ABSTRACT TO THE DISSERTATION

for the degree of Doctor of Law

Specialty: 5.1.5 - International Law Sciences

Scientific consultant:
Doctor of Law,
Associate professor
Razuvaev Nikolay Viktorovich

Moscow - 2025

Federal State Budgetary Educational Institution
institution of higher education
**"RUSSIAN ACADEMY OF NATIONAL ECONOMY
AND CIVIL SERVICE
UNDER THE PRESIDENT OF THE RUSSIAN FEDERATION"**

North-West Institute of Management

On the rights of the manuscript

Alexeyev George Valerievich

LEGAL INTERACTION OF INTERNATIONAL NON-GOVERNMENTAL ORGANIZATIONS AND STATES IN CYBERSPACE

ABSTRACT TO THE DISSERTATION

for the degree of Doctor of Law

Specialty: 5.1.5 - International Legal Sciences

Scientific consultant:
Doctor of Law,
Associate professor
Razuvaev Nikolay Viktorovich

Moscow - 2025

Relevance of the research topic. In the Okinawa Charter on the Global Information Society, adopted on July 21, 2000, developed countries recognize that digital technologies "enable individuals, firms, and business communities to solve economic and social problems more effectively and creatively" (paragraph 1). The Paris Conference on Security and Trust in Cyberspace, held on May 15-17, 2000, recognized the need to ensure the protection of individual freedoms and privacy in cyberspace. Since the beginning of the 21st century, the search for a fair balance in cyberspace between citizen freedom and national security, between the control functions of the state and the liberal aspirations of civil society, has generated active discussions on virtual platforms, within the United Nations system (hereinafter referred to as the UN), and within government structures at the national and supranational levels.

The UN Global Compact of July 26, 2000, evolved from a human rights initiative for sustainable development into an international movement based on the principles of the compact, with its own mission and the socio-economic resources to implement it.

UN General Assembly Resolution No. 79/1 of September 22, 2024, "A Pact for the Future," states the fact: "Digital and emerging technologies, including artificial intelligence, play a significant role as enablers of sustainable development and are fundamentally changing our world" (paragraph 51). The Global Digital Compact, as an annex to the Pact in the name of the future, forms by its legal nature a special act of an international organization of a recommendatory nature - a compact, which all interested actors are invited to recognize and use its provisions to achieve the Sustainable Development Goals (hereinafter - SDGs) proclaimed by the UN General Assembly Resolution of September 25, 2015 No. 70/1 "Transforming our world: the 2030 Agenda for Sustainable Development."

The 2024 Global Digital Compact (hereinafter referred to as the GDC), developed under the auspices of the UN, is based on the concept of multi-stakeholder cooperation (paragraph 17; paragraph 65) for achieving the SDGs , which are also compact in their legal nature. The GDC concept, promoted within the framework of

the UN international cooperation formats, has a number of obvious shortcomings when applied to cyberspace. Firstly, while recognizing the role of private actors in creating what is called *the digital environment* (paragraphs a of paragraph 8), The GDC ignores national interests and proposes that the design of compacts recognize the customs of the virtual world at the discretion of players, which projects legal uncertainty into the economic space of the digital network.

Research into the legal interactions between the state and international civil society institutions in cyberspace is of interest due to the noospheric and cultural opportunities that digital technologies and network platforms offer to citizens, corporations, states, the entire international system, and every household. The role of the state in cyberspace depends not only on its extraterritorial jurisdiction and the capabilities to implement DGPT in the national economy, but also on the strategic readiness of state institutions and the UN for constructive international communication in a modern digital format.

In Russian legal science, issues of the theory of international law have been thoroughly studied in the works of such scholars as: A.Kh. Abashidze, L.P. Anufrieva, G.M. Velyaminov, E.V. Vinogradova, A.N. Vylegzhanin, L.N. Galenskaya, S.A. Egorov, G.V. Ignatenko, R.A. Kalamkaryan, A.Ya. Kapustin, S.Yu. Kashkin, V.P. Kirilenko, Yu.M. Kolosov, I.I. Lukashuk, S.A. Malinin, I.S. Marusin, B.R. Tuzmukhamedov, G.I. Tunkin, I.Z. Farkhutdinov, S.V. Chernichenko and others.

The issues of the status of non-governmental organizations in the modern international system and the problems of international information law are thoroughly examined in the works of such authoritative lawyers as: A.I. Abdullin, V.V. Arkhipov, E.E. Ampleeva, Yu.G. Babaeva, A.A. Danelyan, V.V. Denisenko, A.A. Dorskaya, O.V. Zaitsev, M.B. Kasenova, M.V. Majorina, D.A. Pashintsev, I.V. Ponkin, V.N. Rusinova, V.P. Salnikov, S.L. Sergevnin, D.P. Strigunova, V.P. Talimonchik, A.M. Tarasov, L.V. Terentyeva, G.P. Ermolovich, I.N. Lebedinets, S.V. Maslova, Yu.V. Mishalchenko, I.A. Orlova and others.

Various aspects of the status of private actors in the modern international system are raised in the works of famous Western scholars, including: Jean d'Aspremont, Barry E. Carter, Steve Charnovitz, James Crawford, Duncan B. Hollis, Matthew Parish, August Reinisch, Malcolm Nathan Shaw, Finn Seyersted, Daniel Thurer, Allen S. Weiner, and others. Various aspects of modern international information law are explored by such legal scholars as: Susan J. Drucker, Jacqueline Eggenschwiler, Gary Gumpert, Joanna Kulesza, Lester Lawrence Lessig III, Michael L. Rustad, Hannibal Travis and others.

The purpose of the study: to develop a framework for international legal interaction between states and non-governmental organizations to ensure sustainable development and international information security, establish legal defense of the digital environment from cybercrime and propaganda of violent extremism, and to provide protection for national interests, safety and sovereignty of the Russian Federation in cyberspace.

Achieving this goal requires solving a set of research tasks:

- to model the legal order of international cyberspace suitable for achieving sustainable development goals and ensuring the national security of states;

- to define the status of non-governmental organizations in cyberspace, to formulate and define the content of the concept of "digital freedom" in relation to the activities of INGOs;

- to identify and to formulate special international legal principles for interaction between INGOs and the state in cyberspace, and to justify the need for broad recognition of such principles;

- to develop a concept of digital rights, where their emergence and implementation is possible with the assistance of states, international non-governmental organizations and transnational corporations in the distribution of digital assets;

- to propose an original classification of INGOs, characterizing their missions, tasks and functions that determine the rules of their interaction with the state in cyberspace;

- to define the concept of "virtual INGOs" and characterize their organizational and legal forms used in interaction with the state to ensure security, freedom and trust in cyberspace;

- to develop a concept of virtual competence and substantiate the rationality of states recognizing the virtual competence of INGOs;

- to clarify the content of the concept of "digital sovereignty of the state" and to characterize the system of its provision when interacting with various types of non-governmental organizations;

- to provide an international legal qualification for the participation of non-governmental organizations in operations against the national interests of states in cyberspace;

- to propose a new methodology for international legal regulation for resolving conflicts arising as a result of legal interaction between states and international non-governmental organizations in cyberspace;

- to characterize the transnational rules of interaction between states and non-governmental organizations in cyberspace and justify the need for exceptions to them for the purposes of sustainable development and the protection of the national interests of the Russian Federation;

- to justify the need for states to maintain functional lists, lists and registers of international non-governmental organizations to protect digital sovereignty;

- to formulate proposals for modernizing the system of international legal support for information security in the interaction of the state and non-governmental organizations with the participation of artificial intelligence (AI) agents;

- to prove the influence of digital values and technologies on the formats of interaction between the state and non-governmental organizations;

- to form a constructivist understanding of the legal force of legal acts of international non-governmental organizations in cyberspace and characterize *the legal framework for the recognition* of such acts by states;

- to formulate proposals for the development of formats for legal interaction between government agencies and international non-governmental organizations in

the process of international legal support for the national interests of the Russian Federation.

Object and subject of research.

The research focuses on the legal conditions and legal practices of interaction between influential international non-governmental organizations and states in a virtual environment created by digital technologies. **The dissertation** examines the functional system of contractual and customary norms of transnational law that underpins trust, freedom, and security in cyberspace, as well as international legal guarantees of the integrity and security of the Internet in interactions between states and civil society organizations.

The scientific novelty of this work lies in its substantiation of the strategic importance of legal interaction between the state and international non-governmental organizations for the sustainable development of cyberspace. The originality of the study is determined by its doctrinal approach to international legal interaction as a format for constructive and emergent international communication between the state and representatives of progressive civil society for the common good, based on trust, republican principles, and values.

1. The author presents the construct of *"cyberspace,"* where developed states, international non-governmental organizations (INGOs), and transnational corporations (TNCs) recognize the international status (regime) of the virtual environment as a result of the introduction of digital technologies into the national economy. The legal framework of cyberspace is characterized, where, in various formats and frames, the promotion of sustainable development, the fight against crime, and competition for digital assets are realized—that is, *legal interactions* between players occur. Using thematic analysis, it is demonstrated that the jurisdiction of states and the competence of INGOs in the digital environment are shaped by the norms *of ordinary cyberspace law.*

2. The doctrinal basis *of fiduciary constructivism has been developed* – a new legal approach to understanding the modern international system, which considers freedom, trust and security as a necessary and complementary set of legal

conditions, under which narrative analysis and phenomenological reduction allow us to establish the existence of global cyberspace as a necessary functional transnational and noospheric system of international legal interaction.

3. The principle *of democratic leadership and trust* in cyberspace is formulated, and the legal conditions under which the fiduciary function of INGOs is ensured by their consultative status in the UN system or achieved through the actual mobilization of intellectuals to address heuristic challenges in legitimizing the architecture of cyberspace and maintaining its unity, freedom, and security are outlined. The process of establishing sovereign national segments of global cyberspace through legal means is described, which is impossible without the actual interaction of states and INGOs.

4. The missions and legal acts of INGOs are presented as a system of transnational legal sources, analyzed comparatively, and systematized. INGO missions not only determine the consultative status of INGOs within the UN system but also shape the latent functional legal personality of INGOs within the cyberspace framework. INGO acts determine the trust placed in their projects and leaders by the international community. The fiduciary nature of legal interaction in cyberspace is reflected in the development of formats for cooperation and competition between states, transnational corporations, and INGOs in the digital environment.

5. The virtual competence of INGOs has been identified, which is explained by the leading positions of collective private entities in the implementation of digital innovations and their ability to carry out unilateral legal acts that are recognized *as law-forming legal facts when interacting with developed countries.*

6. The author proposes a definition *of digital sovereignty* based on the rational need to utilize the constructs of international movements to implement the state's extraterritorial jurisdiction in the transnational digital environment within the framework of the general principles of public international law. A number of practical proposals for improving the Russian Federation's policy toward INGOs are formulated.

7. The article characterizes various criminal manifestations of the digital environment as a result of a deficit in *the system of strategic trust (trust – confidence – distrust)* and shows how *a complex of errors in network trust or trust by mistake (mistrust)* leads to anomie in cyberspace and international conflicts.

The validity and reliability of the research results are determined by its broad, representative information base, consistent with the goals and objectives of the methodology, citations of authoritative Russian and foreign scholars, international agreements, regulatory legal acts, corporate documents, case law materials and other sources, and testing in publications and presentations at scientific and practical events at the national and international level.

The provisions submitted for defense and having scientific novelty:

1. A model of legal interaction between International Non-Governmental Organizations (INGO) and the State has been developed. This model allows for: (1) the development and coordination of rules for the functioning of universal digital platforms between players through INGO missions under the jurisdiction of developed states, (2) consultations between states and INGOs within the UN system for the international legal protection of the digital environment, and (3) the systematic implementation of INGO competence in liberal, diplomatic formats on Internet platforms where communication occurs in accordance with the general principles of international law, based on trust and agreed rules. A thematic analysis is used to demonstrate that such fiduciary cyber interaction has become part of the factual and axiological basis of the Rule-Based International Order (RBIO). The article describes typical models of international legal relations within the RBIO framework, which have formed an international system of digital assistance. Foreign relations agencies and other humanitarian structures of developed countries, such as Rossotrudnichestvo, can assume obligations and provide assistance to developing countries in overcoming all forms of the digital divide in accordance with the obligation of states to cooperate with each other and the principle of non-interference in matters within the domestic jurisdiction of states. (paragraphs 3, 5, 21, and 29 of the scientific specialty passport 5.1.5. "International Legal Sciences").

2. The basic nature of the international legal concept of "cyberspace" is substantiated, which is defined as an area of the digital environment with a transnational legal regime, where the principles of international cooperation and the protection of human rights, subject to mutual trust between developed states and INGOs, as well as the conscientious fulfillment by these players (actors) of obligations in accordance with international law, lead to the development of digital international formats and functional legal frameworks that ensure the fair protection of national and corporate interests as a result of the distribution of digital assets and the protection of the right of access to digital platforms; at the same time, the fundamental obligation of states to cooperate with each other in accordance with the UN Charter (clause 3 of Article 1, Article 56) guarantees developing states the right to access digital technologies and the resources of cyberspace, while all INGOs receive access to the resources of the digital environment based on their own missions, with respect by the world community for the principle of the protection of human rights and digital freedom.

A theoretical framework for constructivism, based on trust-based interactions between public and private actors (fiduciary constructivism), has been developed. This framework characterizes the rules of interaction between players on digital platforms in such a way that, within the framework of the principle of legality, an emergent transnational environment of digital freedom, cybersecurity, and strategic trust arises. In a most-favored-nation regime under the jurisdiction of developed countries, INGOs distribute digital assets according to rules, resulting in all those participating in trusted digital communication acquiring subjective digital rights and obligations protected by law.

The concept of digital liberty has been formulated as a legal condition under which the technological capabilities and the ability of states and international non-governmental organizations, supported by the principles of international law, to create digital platforms and assets in accordance with their constitutions and missions, as well as to use the resources of cyberspace available to them in any manner not prohibited, have been established. (paragraphs 2, 3, 5, 29 of the Passport

of the scientific specialty 5.1.5. "International Legal Sciences")

3. It has been proven that the balanced action of the general principles of the sovereign equality of states and the protection of human rights allows states, when interacting with INGOs implementing digital development strategies and operating within the framework *of the Rule-Based Order in Cyberspace (RBOCS)*, to create secure platforms under national jurisdiction. Based on an analysis of the influence of the general principles of international law on the interaction of states and INGOs online, the following special principles of cyber interaction have been formulated: (1) the protection of digital rights, (2) the legality and obligation to assist in the fight against ordinary cybercrime, (3) the indivisibility of cybersecurity, (4) democratic leadership and strategic trust in the Internet. The need for broad international recognition of such principles is substantiated, given that all cyberspace platforms are subject to them in order to maintain trust and digital freedom in the RBOCS formats and frames. (paragraphs 3, 5, 6, 12, 29 of the Passport of scientific specialty 5.1.5. "International legal sciences")

4. Using comparative legal research and participant observation, we demonstrate that states protect digital sovereignty and ensure information security within the RBOCS framework through political and legal means at all levels of the international system, with the participation of *non-governmental organizations (NGO)*. We demonstrate how the leadership of *government operated NGO (GONGO)*, the compliance of their missions with the principles of international law, and the strategic trust of foreign states and international organizations influence not only the legal status of GONGOs but also the digital sovereignty of states interested in the success of their declared missions.

In the author's definition, digital sovereignty is understood as the state's ability, ensured by national legislation, digital technologies, hardware, cultural and diplomatic potential: (1) to implement an information security strategy independent of the interests of foreign elites, based on assisting the missions of leaders in the digital environment, (2) to practice extraterritorial jurisdiction in cyberspace with the help of INGOs within the framework of the principles of international law, (3)

to recognize the emergent digital capabilities of virtual communities and use them in national interests. (paragraphs 3, 4, 5, 27, 29 of the Passport of scientific specialty 5.1.5. "International Legal Sciences").

5. Through participant observation and a comparative legal analysis of INGO acts, the transnational legal capacity of states and INGOs in cyberspace is revealed. It is conditioned by the existence of legally enforceable digital obligations and opportunities for all players to exercise real and virtual digital rights. In the proposed author's classification, real digital rights are associated with the creation and maintenance of the uninterrupted operation of the technical infrastructure of the Network, as well as with actual access to the resources and benefits of cyberspace; real digital rights are exercised by players under the jurisdiction of the state or in spaces with an international regime and generate privileges for individuals; virtual rights are secondary to real rights in the sense that they do not receive jurisdictional protection from the state without the recognition of real digital rights by the state; virtual rights exist in the form of digital code only under the condition of the Network functioning according to the rules and are exercised by all actors (players) on its platforms. It has been proven that ensuring access to the Internet, that is, creating conditions for the implementation of real digital rights for everyone, has become the responsibility of a modern legal and democratic state within the framework of the RBIO and §10 of the Global Digital Compact of 2024 (paragraphs 3, 5, 12, 29 of the Passport of the scientific specialty 5.1.5. "International Legal Sciences").

6. Based on an analysis of the rules of fiduciary cyber interaction, the classification of INGOs has been refined. Informal *international organizations with only virtual competence (VINGOs – Virtual INGOs)* are identified as a separate group. VINGOs include virtual communities, social and volunteer movements, such as digerati and cryptoactivists. Practices of fulfilling VINGO missions and achieving strategic goals through the exercise of their virtual competence have been identified. While VINGOs are not tied to a specific jurisdiction or legal form, they successfully implement their missions online through creative unilateral actions, provided the

internet community trusts their leaders and emergent initiatives.

Virtual competence is defined as the inherent ability of digital communities to participate in the governance of Internet platforms, create rules for the distribution of digital assets, and perform creative or heuristic legally significant actions in cyberspace to implement digital real and virtual rights while fulfilling missions reflected in their founding acts (constitutions), including programmatic declarations and rules (white papers). The ability of informal digital communities and movements to confidentially perform productive, creative acts is demonstrated, which over time will lead to an understanding of the role of robotics in the global community and the recognition by players of legal acts of artificial intelligence (AI) agents as law-making actions. It is proven that AI agents developed and administered by international quasi-organizations can be recognized by states as actors – bearers of virtual competence. (paragraphs 3, 5, 29 of the Passport of Scientific Specialty 5.1.5. "International Legal Sciences").

7. The article outlines the formats of contemporary legal interaction between states and INGOs under the auspices of the UN and its specialized agencies, which mediate the political and economic missions of INGOs in cyberspace. The global environment of digital freedom is modeled as a series of interconnected functional systems and legal frames of RBOCS: (1) a cognitive system in interactive and mediative content frames, (2) a creative system in intellectual frames, (3) an economic system in axiological frames, (4) a technical system of interface frames. It is proven that, as a result of the mediatization of power in the digital environment, special principles, rules, and norms of transnational law have been formed, ensuring the implementation of digital rights and obligations of actors in the RBOCS frames that have developed in the functional systems of cyber interaction. (paragraphs 3, 5, 12, 29 of the Passport of the scientific specialty 5.1.5. "International Legal Sciences").

8. In the context of legal support for information security, the rationality of granting state bodies the competence to interact with international non-governmental organizations (INGOs) to legitimize methods of combating cybercrime and the

promotion of violent extremism within the framework of international law is substantiated. It has been proven that criminal communities are capable of exploiting aberrations in online trust (mistrust) to achieve their criminal goals. A comparative legal analysis shows that a lack of trust (confidence) between developed countries and the global human rights movement leads to international conflicts in cyberspace (information wars). In the context of information confrontation between developed countries, the rationality of organizing international cooperation between the Russian Federation and INGOs to counter cybercrime and violent extremism at the regional level, for example, within the framework of the CIS, EAEU, and SCO, is argued. (paragraphs 25, 27, 29 of the Passport of scientific specialty 5.1.5. "International Legal Sciences").

9. The international legal classification of aggressive operations in cyberspace, characterized within the metadiscourse of "information warfare," as a system of unfriendly actions and counter-retorsions based on competition and mutual distrust among players is substantiated. This means that within the framework of RBOCS, states, transnational corporations (TNCs), and INGOs do not recognize the principle of reciprocity but have the capacity for an asymmetric response in protecting their interests and digital rights. The UN Security Council is encouraged, in accordance with the principle of the indivisibility of information security, to establish a working format for responding to unfriendly operations by states and INGOs in cyberspace. The threats and challenges of digital platform dysfunction and online anomie are substantiated, and to overcome these, developed states have the right to create and reorganize INGOs with missions to harmonize cyberlaw, protect digital sovereignty, and ensure a state of international trust and cybersecurity. (paragraphs 2, 3, 5, 27, 29 of the Passport of scientific specialty 5.1.5. "International legal sciences").

10. It has been demonstrated that the jurisdictions of developed countries provide most-favored-nation treatment for constructive VINGOs—creative communities and digital AI platforms. The rationale for developed countries to maintain preferential treatment within the national digital environment for INGOs

with constructive transnational missions and socially beneficial goals is substantiated, as the sustainable development of cyberspace requires mutual trust between states and INGOs. It has been revealed that national securitized segments of cyberspace are created through the mandatory restriction of real digital rights. It is proposed, in the Russian national interest to ensure the unity of the Eurasian economic and information space, to agree on a mandatory transnational procedure for access to Internet resources and its virtual platforms at the level of integration associations of states (the CIS, the EAEU, and the Union State) and to technically ensure its compliance by establishing a competent and independent INGO. (paragraphs 4, 6, 29 of the Passport of scientific specialty 5.1.5. "International legal sciences").

11. A mechanism for international legal regulation of transnational relations in functional systems of fiduciary cyber interaction, where lawmaking takes place and industry-specific cyberspace frameworks are formed, has been developed. The need for public authorities to consult with leaders of the national and international internet community to achieve consensus on addressing the radicalization of internet discourse is argued, and how sovereign, yet unfounded, prohibitive regulation leads to digital divides is demonstrated. As a result of the thematic analysis, the "Internet Society" is characterized as a global social movement. It is argued that the diplomatic work of the "Russian Internet Society" in the national interest will facilitate a trusting dialogue within the human rights system of international non-governmental organizations (INGOs) under the auspices of the UN and the socio-technical system of international non-governmental organizations (INGOs) formed around the Internet Corporation for Assigned Names and Numbers (ICANN).

The Internet Engineering Task Force (IETF) has been proven to possess virtual competence within the ICANN legal system due to the recognition of its mission within interface frames by all actors (players) in the creative and economic systems of cyber interaction. Within the digital assistance system, a number of *technical assistance NGO (TANGO)* have been identified that are competent in the technical system of cyberspace and are obligated to assist developing countries in

bridging the digital divide, ensuring cybersecurity, and strategic trust in digital technologies. (paragraphs 3, 5, 11, 25, 29 of the Passport of Scientific Specialty 5.1.5. "International Legal Sciences").

12. Based on a comparative legal analysis of INGO missions, a system of sources of transnational cyberspace law has been developed. It has been demonstrated that the recognition by developed countries of the legality of the emergent results of creative unilateral acts of INGOs in the formats and frames of cyber interaction has become the core of RBOCS. Regulatory legal acts of INGOs have been identified that are qualified by the international community and individual states as law-forming legal facts, provided that they comply with the special principles of cyber interaction. It has been demonstrated that the lack of an organizational and legal form for VINGOs does not preclude state recognition of their status and virtual competence; at the same time, the protection of the digital rights of virtual communities under a specific jurisdiction depends on mutual trust between each of them and the state. (paragraphs 2, 3, 5, 6, 8, 21, 29 of the Passport of scientific specialty 5.1.5. "International Legal Sciences").

13. Legal relations online are presented as acts of mutual trust, meaning that most actions by players to exercise virtual rights are fiduciary in nature, leading to digital diplomacy. It has been demonstrated that the "persona grata" status of INGOs within the UN system allows them to enjoy privileges in cyberspace and most-favored-nation treatment under friendly jurisdictions. It is proposed, in the interests of ensuring national information security, to grant the Russian "People's Diplomacy" movement, through the rhizomatic network of INGOs, broader virtual competence and to ensure international trust in its democratic leadership. The rationale for opting for state accreditation of a specific INGO and recognition of its virtual competence in the subject field of diplomatic law is substantiated, given that the INGO's mission coincides with the national interests of all developed countries. (paragraphs 2, 3, 5, 11, 29 of the Passport of Scientific Specialty 5.1.5. "International Legal Sciences").

14. Using game theory methods applied to transnational cyberlaw institutions, the need to protect freedom of speech, legally prohibit censorship, and hold

extremists accountable for defamation in cyberspace is demonstrated for the creation and implementation of platform law in international non-governmental organizations (NGO) trusted by developed countries. The need to protect the intellectual and digital rights of members of Russian and international *scientific and creative unions (TUNGO – Trade Union NGO)* through joint efforts by CIS member states and civil society to re-establish the International Organization of Journalists (IOJ) and promote its mission is substantiated. (paragraphs 2, 5, 12, 29 of the Passport of Scientific Specialty 5.1.5. "International Legal Sciences").

15. Frames have been identified in functional systems of cyber interaction—frames within which players recognize rules and develop institutions of transnational cyberspace law. Cognitive frames of cyberspace have been identified that legitimize rules, for example, in the field of sports law (lex sportiva), and corporate creative frames of international private law, such as advertising law, entertainment law, fashion law, etc. (paragraphs 2, 3, 5, 6, 8, 29 of the Passport of Scientific Specialty 5.1.5. "International Legal Sciences").

16. A thematic analysis of RBOCS corporate frames revealed the use of language games to legitimize interaction rules and exceptions. The role of the digital assistance system in TNC policies to implement the creative and axiological frames of RBOCS through specialized UN agencies and *BIg INGO (BINGO)* into the national legal systems of developing countries is determined. It is proven that free access to software and Internet content is the foundation of RBOCS; that is, real digital rights can be unfairly limited by intellectual frames or interface hardware, as well as by defective prohibitive norms of national legislation. This requires (in return) maintaining trust between states and INGOs competent in resolving disputes over digital assets and rights. (paragraphs 2, 5, 29 of the Passport of the scientific specialty 5.1.5. "International Legal Sciences").

17. A framing analysis of RBOCS values demonstrated the need for international recognition and cross-border distribution of digital assets to effectively protect digital rights. It has been demonstrated that competition in the digital asset market requires state recognition and legal protection of digital rights. However,

trust in the axiological framework of transnational cyberspace law, for example, in the field of cryptocurrencies, depends on the method of digital asset distribution and presupposes a lack of competence among players to change the rules of interaction without their consent. This leads to automated protection of digital rights by VINGO and the operation of AI platforms outside the national jurisdiction of states. (paragraphs 3, 5, 29 of the Passport of Scientific Specialty 5.1.5. "International Legal Sciences").

18. Trust-based legal interaction between states and INGOs in cyberspace is conceptualized through: (1) assistance from civil society leaders and government bodies to ensure digital freedom and security in the implementation of digital rights under the national jurisdiction of developed countries, (2) regulated and legally protected competition between digital TNCs and other competent players in the digital asset market, and (3) the players organizing counteraction to cybercrime, propaganda of violent extremism, interference in matters within the domestic competence of states, and other manifestations of destructive cyberactivity. (paragraphs 2, 3, 5, 29 of the Passport of scientific specialty 5.1.5. "International Legal Sciences").

Practical significance of the study. In the modern international system, strategic formats for interaction between states and INGOs pursue the goals of sustainable development and ensure the security of cyberspace for all. Prohibitory legal regulation has become a strategy of developed countries to protect the national segment of cyberspace from extremism and cybercrime. A comprehensive legal analysis shows that national and corporate regulatory lists of accredited INGOs are necessary to ensure the information security of the state and maintain legal certainty under national jurisdiction. In order to ensure international strategic trust in the Russian state, the Ministry of Justice of the Russian Federation is proposed to regulate the procedure for working in cyberspace with INGO resources that have consultative status with the UN and organize constructive work on the administration of the following documents: (1) The register of INGOs enjoying most favored nation status - the "white list", (2) The list of INGOs performing the

functions of foreign agents - the "diplomatic list", (3) The list of agents interfering in matters within the domestic competence of the state, extremist and criminal communities - the "black list". When developing rules for cyber interaction with INGOs from the "diplomatic list" under Russian jurisdiction, such work to ensure national security must be coordinated with the Ministry of Foreign Affairs of the Russian Federation.

Research Results Approval. The author's key findings from the dissertation are reflected in 93 publications, including 7 monographs and over 70 articles in peer-reviewed journals recommended by the Higher Attestation Commission under the Ministry of Science and Higher Education of the Russian Federation for publication of the main research results of dissertations for the degrees of candidate of science and doctor of science (including 7 articles in journals included in the international citation databases Scopus or Web of Science and 17 articles in peer-reviewed journals recommended to specialty 5.1.5. "International Legal Sciences"). The dissertation materials were tested in the author's presentations at over 50 scientific events of various levels, including 25 international ones.

The author participated in the development of the provisions of the Convention on the Preservation of Cultural Heritage Sites of the Commonwealth of Independent States Member States of November 27, 2020, and the model laws of the Interparliamentary Assembly of Member Nations of the Commonwealth of Independent States "On Combating Cybercrime" and "On Engineering", as confirmed by the Act on the Practical Use of Research Results provided by the Secretariat of the Interparliamentary Assembly Commonwealth of Independent States Council.

The applicant's scientific ideas have found application in textbooks on integration and maritime law, which are used by muster students at the North-West Institute of Management, a branch of the Russian Presidential Academy of National Economy and Public Administration.

The dissertation's structure is determined by its purpose, objectives, the author's concept of studying legal interactions at the international level, and the

research methodology and information base. The work consists of an introduction and two sections, the first of which includes three chapters, and the second two chapters. All five chapters are divided into four paragraphs. The work also contains chapter conclusions, nine figures, and two tables. The conclusion provides conclusions and recommendations. The study includes a list of key abbreviations, a reference list, and a bibliography comprising 668 titles.