

International cooperation on information security

NURMAN SEIDAKMATOV

State committee for national security of the Kyrgyz Republic, lieutenant general

A.K Bakayev academy, Bishkek, Kyrgyz Republic

Email: nurkg72@mail.ru

ARTICLE INFO

Article History:

Received July 2, 2026

Revised July 6, 2026

Accepted July 10, 2026

Available online July 12, 2026

Keywords:

information security;
international law;
cyberspace;
Kyrgyz Republic;
CSTO;
SCO;
CIS;
UN
GGE;
OEWG;
cyber diplomacy.

Correspondence:

E-mail: nurkg72@mail.ru

ABSTRACT

The globalization of information and communication technologies (ICTs) has transformed information security from a purely domestic concern into a matter of international law and multilateral diplomacy. This article examines the current state of international law in the information sphere, its prospects for development, and the extent to which it shapes the information security policy of the Kyrgyz Republic. The article further analyses the concrete forms and channels through which the Kyrgyz Republic participates in international legal cooperation on information security, including the United Nations, the Commonwealth of Independent States (CIS), the Collective Security Treaty Organisation (CSTO), the Shanghai Cooperation Organisation (SCO), and the Eurasian Economic Union (EAEU). The study relies on comparative-legal and systemic analysis of international treaties, resolutions, and doctrinal sources, and concludes with recommendations for strengthening the normative and institutional basis of Kyrgyzstan's participation in the global information security regime.

1.Introduction

Information security has become one of the central issues of contemporary international relations. The rapid expansion of digital infrastructure, the growing dependence of states on ICTs, and the corresponding rise of cross-border threats — cyberattacks, disinformation campaigns, digital espionage, and the malicious use of ICTs by state and non-state actors — have made purely national approaches to information security insufficient [1], [4]. Ensuring a stable, predictable, and rules-based information space requires coordinated action at the bilateral, regional, and universal levels.

For the Kyrgyz Republic, a landlocked state in Central Asia with a comparatively modest domestic capacity for independent technological development, international legal cooperation is not a supplementary option but a structural necessity. Kyrgyzstan's information security is shaped as much by treaties, resolutions, and regional agreements to which it is a party as by its own domestic legislation [2], [7]. This article therefore addresses two closely related questions: first, what is the current state and trajectory of international law governing the information sphere, and how does it influence Kyrgyzstan's

information security; second, through which concrete institutional forms does the Kyrgyz Republic realize its participation in this legal cooperation.

1. MODERN INTERNATIONAL LAW IN THE INFORMATION SPHERE: CURRENT STATE, PROSPECTS, AND INFLUENCE ON THE INFORMATION SECURITY OF THE KYRGYZ REPUBLIC

1.1. The Formation of a Normative Framework for State Behaviour in Cyberspace

Unlike traditional domains of international law, the information sphere lacks a single, universally binding treaty comparable to the law of the sea or the law of armed conflict. Instead, the applicable normative framework has emerged incrementally through United Nations mechanisms, principally the Groups of Governmental Experts (GGE) convened between 2004 and 2021, and the Open-Ended Working Groups (OEWG) that operated from 2019 to 2025 [3], [5]. The consensus GGE reports of 2010, 2013, 2015, and 2021 progressively affirmed that existing international law, including the UN Charter, applies to state conduct in cyberspace, and the 2015 report enumerated eleven voluntary, non-binding norms of responsible state behaviour [5], [9].

The concluding report of the second OEWG, adopted in July 2025, consolidated these achievements and established a permanent successor mechanism — the Global Mechanism on developments in the field of ICTs in the context of international security — tasked with continuing negotiations on norms, confidence-building measures, capacity-building, and the applicability of international law within a single-track, universal format [5], [9], [11]. This evolution signals a shift from ad hoc expert consultations toward a more institutionalized, if still largely non-binding, regime, sometimes referred to informally as the emerging 'acquis' of responsible state behaviour in the use of ICTs [5].

1.2. Competing Doctrinal Approaches and Unresolved Questions

The prospects for further development of international law in this sphere remain contested along two axes. The first is the divide between states advocating a binding international treaty on information security — a position historically associated with the Russian Federation since its 1998 proposal to the UN First Committee — and states, primarily Western, that favour the application of existing international law supplemented by voluntary norms and confidence-building measures [8], [9]. The second unresolved question concerns the precise modalities of applying international humanitarian law, the law of state responsibility, and the principle of due diligence to ICT-related incidents, given the difficulties of attribution and the prevalence of operations conducted in the so-called 'grey zone' between criminal and inter-state activity [11].

For a state such as Kyrgyzstan, which does not possess independent offensive cyber capabilities and is primarily concerned with defensive resilience, the practical significance of this doctrinal divide lies less in abstract legal theory and more in the availability of capacity-building assistance, technical standards, and confidence-building measures that regional and universal mechanisms can offer to developing states [10].

1.3. Regional Legal Instruments and Their Interaction with Universal Norms

Alongside the UN-centred process, several regional organisations of which Kyrgyzstan is a member have adopted their own instruments addressing information security, most notably the 2009 SCO Agreement on Cooperation in the Field of International Information Security and successive CSTO and CIS agreements on cooperation in combating offences in the information sphere [2], [7]. These regional instruments generally adopt a broader conception of 'information security' than the Western notion of 'cybersecurity,' encompassing not only the technical protection of ICT infrastructure but also the content

dimension of information exchange, including concerns about the use of ICTs for interference in internal affairs [7], [8]. Table 1 summarizes the principal international and regional legal instruments relevant to the information security of the Kyrgyz Republic.

Table 1. Principal international legal instruments relevant to information security and Kyrgyzstan's involvement

Instrument / Mechanism	Level / Year	Core content relevant to information security	Status for Kyrgyzstan
UN GGE Reports (2010–2021)	Universal, UN	Affirms applicability of international law and the UN Charter to ICT use; 11 voluntary norms of responsible behaviour	Participates via UN membership since 1992
UN OEWG Final Report / Global Mechanism	Universal, 2021–2025	Establishes a permanent, single-track institutional process; confidence-building measures; capacity-building	Participates as UN member state
SCO Agreement on International Information Security	Regional, 2009	Broad concept of information security; cooperation against 'information weapons' and destabilizing content	Ratified; SCO member state
CSTO Cooperation Agreements on Information Security	Regional, CSTO	Coordination of information security policy among member states; joint response to threats	Member state; chaired CSTO in 2013
CIS Agreement on Cooperation in Combating Offences in the Information Sphere	Regional, CIS	Harmonization of legislation; mutual legal assistance in ICT-related offences	Member state, ratified
Budapest Convention on Cybercrime (Council of Europe)	Regional/open for accession, 2001	Criminalization of cybercrime; procedural and mutual assistance mechanisms	Not a party; referenced as a comparative model

1.4. Influence on the Domestic Information Security Policy of the Kyrgyz Republic

The influence of these international instruments on Kyrgyzstan's information security policy is threefold. First, they provide the doctrinal vocabulary and conceptual framework — 'information security,' 'critical information infrastructure,' 'responsible state behaviour' — that has been transplanted into national strategic documents and legislation [2], [7]. Second, participation in regional agreements creates concrete obligations to harmonize domestic law with the standards adopted collectively, most visibly in the areas of personal data protection and combating cybercrime, where Kyrgyzstan has established a dedicated State Agency for the Protection of Personal Data [7]. Third, membership in these bodies opens access to capacity-building programmes, joint exercises, and technical assistance that domestic resources alone could not provide, including CSTO coordination councils on emergency and information-security cooperation [4], [7].

At the same time, the non-binding character of most universal norms and the absence of a comprehensive treaty leave considerable room for divergent national interpretations, which constrains the predictability of the international legal environment within which Kyrgyzstan must operate. This suggests that, for the foreseeable future, Kyrgyzstan's information security will be shaped by a plurality of overlapping regional and universal frameworks rather than by a single, coherent global regime [5], [11].

Findings of Chapter 1

The analysis shows that international law in the information sphere is still in the process of formation, developing through a combination of universal UN mechanisms and regional treaty regimes rather than through a single comprehensive convention. For the Kyrgyz Republic, this fragmented but expanding normative environment functions simultaneously as a source of doctrinal orientation, a channel for capacity-building, and a constraint arising from legal uncertainty, making active participation in international legal cooperation indispensable to the country's information security.

2. WAYS AND FORMS OF THE KYRGYZ REPUBLIC'S PARTICIPATION IN INTERNATIONAL LEGAL COOPERATION ON INFORMATION SECURITY

2.1. Participation Through Universal Organisations

As a member of the United Nations since 1992, the Kyrgyz Republic participates in the universal track of information security cooperation primarily through its voting and consultative role in the UN General Assembly's First Committee processes, including the submission of national views to the Secretary-General on developments in the field of ICTs in the context of international security, and through engagement with the Global Mechanism established following the 2025 OEWG Final Report [3], [9], [10]. This channel gives Kyrgyzstan access to the broadest possible normative discussion, though its practical influence on outcomes is necessarily limited by the country's modest diplomatic and technical resources relative to major cyber powers.

2.2. Participation Through Regional and Collective-Security Organisations

The most substantive and operationally significant form of Kyrgyzstan's cooperation occurs at the regional level, through four overlapping organisations: the CIS, the CSTO, the SCO, and the EAEU [2], [7]. Within the CSTO, information security has been treated as a distinct priority area at least since Kyrgyzstan's 2013 chairmanship of the organisation, when countering contemporary challenges and threats, including in the information domain, was named among the chairmanship's stated priorities [1]. The CSTO framework enables joint coordination councils, practical exercises, and exchange of threat information among member states' competent authorities [4].

Within the SCO, Kyrgyzstan is a party to the 2009 Agreement on Cooperation in the Field of Ensuring International Information Security, which frames cooperation broadly to include both technical protection of infrastructure and countering the use of ICTs to destabilize the political and social order of member states [7], [8]. Within the CIS, Kyrgyzstan participates in agreements on combating offences in the information sphere, which are oriented toward harmonizing criminal legislation and enabling mutual legal assistance among CIS members [2]. Within the EAEU, cooperation is centred on the technical and economic dimensions of the digital space, including common approaches to personal data protection and digital trade, which have indirect but significant implications for information security [2].

2.3. Bilateral Treaty Cooperation

In parallel with multilateral engagement, the Kyrgyz Republic has concluded more than one hundred and twenty bilateral treaties, agreements, and other instruments of cooperation with the Russian Federation alone, a portion of which concern security cooperation with direct or indirect relevance to the information sphere [3]. Bilateral cooperation of this kind allows for more flexible and rapid coordination than multilateral frameworks, particularly in the exchange of operational information and joint training of specialists, but it inevitably reflects the asymmetry of capacity between Kyrgyzstan and its larger treaty partners.

2.4. Institutional and Legislative Forms of Implementation

Kyrgyzstan's international obligations are implemented domestically through a defined institutional architecture: the President and the Cabinet of Ministers set overall policy direction, the National Bank participates in matters concerning the security of financial information systems, and the State Agency for the Protection of Personal Data administers compliance with data-protection standards derived in part from international and regional instruments [7]. Table 2 summarizes the principal channels through which Kyrgyzstan participates in international legal cooperation on information security.

Table 2. Forms and channels of the Kyrgyz Republic's participation in international cooperation on information security

Form of cooperation	Organisation / partner	Main content and mechanisms	Level
Multilateral diplomatic engagement	United Nations (First Committee, Global Mechanism)	Submission of national positions; participation in norm-setting discussions and capacity-building	Universal
Collective security coordination	CSTO	Coordination councils; joint exercises; information exchange on threats; 2013 chairmanship priorities	Regional
Regional legal harmonization	SCO	1997/2009 agreements on international information security; countering destabilizing use of ICTs	Regional
Mutual legal assistance	CIS	Agreements on combating offences in the information sphere; legislative harmonization	Regional
Economic and technical integration	EAEU	Common standards for personal data protection and digital trade	Regional
Bilateral treaty cooperation	Russian Federation and other partners	Over 120 bilateral instruments; operational information exchange; joint training	Bilateral
Domestic implementation	State Agency for the Protection of Personal Data; National Bank; Cabinet of Ministers	Transposition of international standards into national legislation and regulatory practice	National

2.5. Limitations and Prospects for Strengthening Participation

Despite this multiplicity of channels, Kyrgyzstan's participation in international legal cooperation on information security faces structural limitations: overlapping and occasionally inconsistent obligations arising from simultaneous membership in the UN, CIS, CSTO, SCO, and EAEU frameworks; a shortage of specialists able to represent the country's interests effectively in technical and legal negotiations; and dependence on partner states for technological capacity [4], [10]. Strengthening Kyrgyzstan's position would require closer alignment of its domestic legislation with the emerging body of international norms, more active use of the capacity-building mechanisms offered by the Global Mechanism and by regional partners, and the development of a coherent national strategy that positions bilateral and multilateral cooperation as complementary rather than competing instruments [9], [10].

Findings of Chapter 2

The Kyrgyz Republic realizes its participation in international legal cooperation on information security through a layered structure combining universal UN engagement, regional cooperation within the CSTO, SCO, CIS, and EAEU, bilateral treaty relations, and domestic institutional implementation. While

this layered approach broadens Kyrgyzstan's access to normative development and capacity-building, it also generates coordination challenges that a more unified national strategy could help to resolve.

3.Conclusion

The article has shown that international law in the information sphere remains a dynamically developing, largely non-binding, but increasingly institutionalized body of norms, anchored in UN GGE and OEWG outcomes and complemented by regional instruments adopted within the SCO, CSTO, and CIS. For the Kyrgyz Republic, this evolving framework shapes domestic information security policy by supplying doctrinal concepts, generating harmonization obligations, and opening channels for capacity-building. Kyrgyzstan's participation in international legal cooperation is realized through a combination of universal, regional, and bilateral forms, implemented domestically through a defined set of state institutions. Strengthening this participation, through greater legislative harmonization and a more coordinated national strategy across the overlapping regional frameworks, would enhance the country's capacity to protect its information space in conditions of persistent global uncertainty regarding the future shape of international law in this domain.

4.References

- [1] Ministry of Foreign Affairs of the Kyrgyz Republic. Kyrgyz Republic and the CSTO: priorities of the 2013 chairmanship. Bishkek, 2018.
- [2] Eurasian Group on Combating Money Laundering and Financing of Terrorism. Kyrgyz Republic: international cooperation profile. 2018.
- [3] Collective Security Treaty Organisation. Kyrgyzstan: country profile. Official CSTO portal, 2026.
- [4] Collective Security Treaty Organisation. From the Treaty to the Organisation: 25 years of the CSTO. Official CSTO portal, 2026.
- [5] Digital Watch Observatory. UN Global Mechanism on Cybersecurity in 2026. Geneva Internet Platform, 2026.
- [6] Baigazieva, A. Information security legislation of the Kyrgyz Republic within the CSTO framework. Information Security Bank Journal, 2020.
- [7] IB-Bank Journal. Review of information security legislation of CSTO member states: the Kyrgyz Republic. 2020.
- [8] Royal United Services Institute. UN norms: tackling the rise of cyber capabilities. RUSI Occasional Paper, 2026.
- [9] CircleID. Breaking ground: historic launch of UN Global Mechanism for cyberspace governance. 2025.
- [10] United Nations Office for Disarmament Affairs. Developments in the field of information and telecommunications in the context of international security. UNODA, 2025.
- [11] Cyber Defense Review. The UN cyber norms: state responsibility, attribution, and the grey zone. U.S. Army Cyber Institute, 2022.
- [12] Just Security. The sixth United Nations GGE and international law in cyberspace. 2021.
- [13] United States Government Accountability Office. Cyber diplomacy: state's efforts aim to support U.S. interests. GAO Report, 2024.

[14] CyberPeace Institute. Advancing the framework of responsible state behaviour in cyberspace. Submission to the OEWG, 2024.

[15] Shanghai Cooperation Organisation Secretariat. Agreement between the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security. 2009.