

How does Russia's victory in the global cyber norms contest reshape the accountability mechanisms and power structures of international digital governance?

September 12, 2026 | SnugLab Research

Executive Summary

Russia's victory in the global cyber norms contest has primarily reshaped accountability mechanisms by institutionalizing state-centric sovereignty as a competing lens for international cyber law, diminishing the role of external attribution. This normative shift, advanced through UN processes and the 2024 UN Cybercrime Convention, allows states to use sovereign jurisdiction as a shield against scrutiny, while simultaneously fragmenting international digital governance into competing jurisdictional silos and fostering dependency among Global South nations through targeted technical assistance. However, this victory is largely procedural and normative, with limited structural enforcement due to low treaty ratification and the continued operational reliance on multi-stakeholder bodies.

Key Findings

Normative Shift Towards State-Centric Sovereignty

Russia has successfully advanced a state-centric vision of cyber sovereignty, reshaping accountability mechanisms by elevating sovereign jurisdiction over external attribution [11]. This approach asserts that state borders extend over cyberspace, granting states the right to control their domestic internet spaces [4, 5, 6, 9, 14]. Through UN processes like the Open-Ended Working Group (OEWG) and the 2024 UN Cybercrime Convention (Hanoi Convention), Russia has embedded principles such as the "inadmissibility of unsubstantiated attributions" [11]. This provision is designed to diminish the importance of state attribution in cyber accountability, effectively creating a high bar behind which state-supported activities can hide [11]. This aligns with Russia's long-standing strategy of using deniable operations for asymmetric influence [1].

Limited Structural Enforcement and Accountability Vacuums

Despite Russia's procedural dominance in UN cyber diplomacy, this has not translated into a durable structural shift of enforcement power to intergovernmental bodies, leading to persistent accountability vacuums [11]. While the UN General Assembly adopted the Hanoi Convention in December 2024, and it opened for signature in October 2025, its final text largely mirrors the Western-backed Budapest Convention rather than adopting Moscow's full authoritarian narrative [11]. As of May 2026, only Qatar, Azerbaijan, and Vietnam have ratified the treaty, with 74 signatories in total, including Tajikistan and Colombia adding their signatures [11]. Major powers like the United States have disengaged, and Western-aligned states, which hold the majority of global electronic evidence, have not joined [11]. Consequently, the UN treaty framework remains practically inaccessible for international cooperation in many cross-border cybercrime investigations, leaving the Budapest Convention as the primary operational mechanism for many nations [11]. Russia's own tendency to violate international law further demonstrates that the core issue is a lack of enforcement rather than a lack of rules [11].

Dual Strategy: Domestic Control and International Ambiguity

Russia employs a dual strategy, using clearly defined territorial sovereignty domestically for control while maintaining international ambiguity to preserve deniability and reshape accountability [1, 4, 5, 6, 8, 9]. Domestically, Russia enforces strict data localization and content filtering. The 2014 Federal Law No. 242-FZ mandates that private internet companies store personal data of Russian users on servers physically located in Russia [8, 10, 16]. The 2019 "Sovereign Internet Law" centralizes control over national infrastructure and requires ISPs to install Deep Packet Inspection (DPI) filtering equipment [8, 10]. Roskomnadzor, Russia's communications watchdog, has actively enforced these laws, blacklisting LinkedIn in 2016 for failing to localize data [3, 8], and compelling Apple to remove 25 VPN apps from its Russia App Store in July 2024 [20].

Internationally, however, Russia strategically maintains ambiguity around sovereignty violation thresholds to shield itself from formal multilateral accountability [11]. Its focus on "information warfare," including disinformation, propaganda, and subversion, relies on deniable and indirect activities that are inherently difficult to attribute [1, 15]. Between 2000 and 2020, approximately 61% of attributed Russian cyber incidents focused on information acquisition rather than disruption [15]. This dual approach allows Russia to dictate the terms of its own accountability, enforcing state control within its borders while exploiting attribution ambiguity to bypass multilateral scrutiny for its external operations [6, 11].

Fragmentation and Dependency in Global Digital Governance

Russia's procedural success is driving a bifurcation of global digital governance, creating competing jurisdictional silos while simultaneously fostering dependency among developing states [11]. As Western states, particularly the United States, have defunded cyber-related capacity-building initiatives linked to the Hanoi Convention, Russia and China are positioned to fill this vacuum [11]. By providing targeted technical assistance to Global South nations, Moscow can tie this aid to support for its state-centric vision of the internet, potentially locking these countries into its accountability framework [11]. Developing countries have shown willingness to back Russian-led initiatives to address structural imbalances and absorb cybercrime costs [11].

However, the lack of universal participation in Russia-backed treaties, particularly the Hanoi Convention, is actively fragmenting the digital governance architecture [11]. The non-participation of Western-aligned states, which hold the majority of global electronic evidence, means that data required for cybercrime investigations will be inaccessible under the UN treaty framework for many nations [11]. This entrenches competing jurisdictional silos, with the Budapest Convention potentially remaining the only practical option for international cooperation among its signatories, while Russia's state-centric track operates separately [11].

Compliance Costs for Multinational Tech Firms

Russia's dual strategy imposes significant and escalating compliance costs and penalty regimes on multinational tech firms. Domestically, Federal Law No. 242-FZ requires data localization, forcing companies to rent local server space [1, 3, 10, 13, 16]. Penalties for localization violations have increased from initial fines of RUB 6,000,000 (approximately \$100,000 USD) to up to 20% of a company's Russian turnover for repeated offenses [10, 17, 19]. Effective May 30, 2025, new regulations impose fines up to RUB 500,000,000 (or 1% to 3% of aggregate revenue) for actions causing a data leak [18]. Beyond monetary penalties, Roskomnadzor enforces compliance through service blocking, as seen with LinkedIn in 2016 [3, 8, 11].

In jurisdictions that have ratified the Hanoi Convention (e.g., Qatar, Azerbaijan, Vietnam), firms face a state-centric compliance environment characterized by broad language and weak human rights safeguards [4, 7, 12]. The Convention requires signatory states to establish liability for legal persons involved in cybercrimes, subject to "effective, proportionate and dissuasive criminal or non-criminal sanctions" [5, 9]. This necessitates

enhanced digital forensics readiness, secure log retention, and cross-border data transfer reviews [17]. Vietnam, for example, mandates local user data storage, content handover to authorities, and 24-hour removal of "illegal" content [2, 7].

Conversely, jurisdictions relying on the Budapest Convention offer clearer legal frameworks with robust human rights protections, judicial oversight, and proportionality requirements [4, 12, 16]. This results in more defined compliance obligations and stronger protections against arbitrary state demands for data or content censorship [12, 16]. However, US-based firms in Budapest-aligned countries face additional complexity from the US CLOUD Act, which can create conflicts of law regarding data disclosure [19].

Implications

Russia's success in the global cyber norms contest implies a significant shift towards a more fragmented and state-controlled international digital governance landscape. Accountability mechanisms are increasingly bifurcated: within state borders, national sovereignty dictates strict data and content controls, while internationally, the principle of "inadmissibility of unsubstantiated attributions" provides a shield against external scrutiny for state-sponsored cyber activities. This dual approach challenges the multi-stakeholder model of internet governance, empowering intergovernmental bodies and authoritarian states to exert greater control over information flows and digital infrastructure. For multinational tech firms, this means navigating a complex and often contradictory regulatory environment, facing escalating compliance costs and legal risks in jurisdictions adopting Russia's state-centric model, while potentially operating under different, more rights-protective frameworks elsewhere. The long-term implication is a less open and more balkanized internet, where geopolitical alignments increasingly determine digital rights and responsibilities.

Limitations and Caveats

The available evidence provides a strong understanding of Russia's normative and procedural successes in shaping international digital governance. However, direct quantitative data on the current market share of state-centric DNS and cloud infrastructure providers in the Global South, compared to Western alternatives, is limited. Similarly, while Russia's intent to use technical assistance to foster dependency is clear, specific, named Russian-led technical assistance programs that have demonstrably

shifted recipient states toward Moscow's state-centric attribution and data sovereignty models, with measurable policy changes, are not detailed in the provided research. Therefore, while the normative and diplomatic shifts are well-supported, the precise structural and infrastructural impacts in the Global South remain less quantified.

Sources

- [1] [gov] Purl - osti.gov - <https://www.osti.gov/servlets/purl/1491981>
- [2] [edu] Varieties Of Digital AuthoritarianismAnalyzing - online.ucpress.edu - <https://online.ucpress.edu/cpcs/article/54/4/1/119028/Varieties-of-Digital-AuthoritarianismAnalyzing>
- [3] [edu] Viewcontent.Cgi - digitalcommons.usf.edu - <https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1134&context=mca>
- [4] [edu] Establishing Cybersecurity Norms In The United Nations The R - hir.harvard.edu - <https://hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/>
- [5] [edu] Anchoring Digital Sovereignty - cjil.uchicago.edu - <https://cjil.uchicago.edu/print-archive/anchoring-digital-sovereignty>
- [6] How Authoritarians Use International Law - journalofdemocracy.org - <https://www.journalofdemocracy.org/articles/how-authoritarians-use-international-law/>
- [7] Research Reports - rand.org - https://www.rand.org/pubs/research_reports/RRA1180-1.html
- [8] [peer-reviewed] Circumventing the "Sovereignization" of the Russian Internet - AUTHORS UNAVAILABLE - <https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/circumventing-the-sovereignization-of-the-russian-internet/20775EC5CCD1DD8930E4B2F58BAD1116>
- [9] CyCon 2021 Pijovic - ccdcoe.org - https://ccdcoe.org/uploads/2021/05/CyCon_2021_Pijovic.pdf
- [10] Reassessing Runet Russian Internet Isolation And Implication - atlanticcouncil.org - <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/>
- [11] Has Russia Overplayed Its Hand In Un Cyber Negotiations - lawfaremedia.org - <https://www.lawfaremedia.org/article/has-russia-overplayed-its-hand-in-un-cyber-negotiations>
- [12] Setting Global Rules In Cyberspace - thecipherbrief.com - https://www.thecipherbrief.com/column_article/setting-global-rules-in-cyberspace
- [13] [preprint] Papers.Cfm - papers.ssrn.com - AUTHORS UNAVAILABLE - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119863
- [14] Russias Great Power Imaginary And Pursuit Digital Multipolar - policyreview.info - <https://policyreview.info/articles/analysis/russias-great-power-imaginary-and-pursuit-digital-multipolarity>
- [15] The Russia Ukraine Conflict From 2014 To 2023 And The Signif - acigjournal.com - <https://www.acigjournal.com/The-Russia-Ukraine-Conflict-from-2014-to-2023-and-the-Significance-of-a-Strategic,184308,0,2.html>
- [16] [edu] Russia Is Weaponizing Its Data Laws Against Foreign Organiza - brookings.edu - <https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/>
- [17] Russia Adopts Increased Fines For Data Protection Violations - hunton.com - <https://www.hunton.com/privacy-and-cybersecurity-law-blog/russia-adopts-increased-fines-for-data-protection-violations>
- [18] Comparative Analysis The Budapest Convention Vs The Un Conve - dig.watch - <https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime>
- [19] [news] Russian Lawmakers Approve Harsher Fines Foreign Tech Firms W - reuters.com - <https://www.reuters.com/world/europe/russian-lawmakers-approve-harsher-fines-foreign-tech-firms-without->

[offices-2022-07-05/](#)

[20] Sovereignty And Data Localization - belfercenter.org -
<https://www.belfercenter.org/publication/sovereignty-and-data-localization>