EUI ACADEMY OF EUROPEAN LAW

AEL 2024/19
Academy of European Law
European Society of International Law Paper

WORKING PAPER

Conceptual Discrepancies in Russian and Western Approaches to International Regulation of Cyber [Information] Space

Liliya Khasanova

European University Institute

Academy of European Law

European Society of International Law
Research Forum, Tartu, April 2023

Conceptual Discrepancies in Russian and Western Approaches to International Regulation of Cyber [Information] Space

Liliya Khasanova

ISSN 1831-4066

Published in August 2024 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu

With the support of the
Erasmus+ Programme
of the European Union

The European Commission supports the EUI through the European Union budget. This publication reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Academy of European Law

The Academy of European Law coordinates several important research projects and offers advanced-level courses, including the annual summer courses in human rights law and the law of the EU, resulting in an extensive publications programme. The Academy also hosts the Secretariat of the European Society of International Law (ESIL), and assists in the organization of ESIL events.
Papers presented at ESIL events in 2011-2019 can be downloaded from SSRN. As of 2022, the papers are available in the EUI CADMUS Research Repository.

More information about the Academy of European Law

European Society of International Law

The European Society of International Law (ESIL) is a dynamic network of researchers, scholars and practitioners in the field of international law. The Society's goals are to encourage the study of international law, to foster inquiry, discussion and innovation in international law, and to promote a greater understanding of the role of international law in the world today. The Secretariat of the Society has been based at the Academy of European Law since 2004 when the Society was set up.

More information about ESIL

ESIL Paper Series

The ESIL Paper Series features papers presented at ESIL events (Annual Conferences, Research Forums, and Interest Groups events). Publication in the ESIL Paper Series enables authors to disseminate their work widely and reach broader audiences without the usual delays involved in more traditional means of publication. It does not prevent the subsequent publication of papers in academic journals or edited collections.

More information about the ESIL Paper Series

2023 ESIL Research Forum, Tartu, 27-28 April 2023

The ESIL Research Forum is a scholarly conference that promotes engagement with research in progress by early-career researchers, who have the opportunity to present their works and receive comments from members of the ESIL Board and invited experts during the Forum. The 2023 ESIL Research Forum was hosted by the University of Tartu on 27-28 April 2023 and addressed the topic "Regional Developments of International Law in Eastern Europe and Post-Soviet Eurasia".

More information about the 2023 ESIL Research Forum

EUI ACADEMY OF EUROPEAN LAW

esil sedi
EUROPEAN SOCIETY OF INTERNATIONAL LAW

Abstract

After more than two decades of ongoing international negotiations aimed at regulating the domain that was created by information and communication technologies (ICTs), it is evident that at least two contradictory approaches have emerged. One notable aspect that has been overlooked is the difference in language used by Russia and Western countries, with Russia referring to ‘information space’ and Western countries using the term ‘cyberspace’. This paper aims to empirically examine this persistent use of different terms related to the ICT ‘space’ and reveal the increasingly contradictory realities that Russia and Western countries are seeking to regulate. To identify the key areas of conceptual discrepancies, I analyse international cyber governance documents and normative proposals from states, national legislations in Russia and Western states, and place them in the historical context of ICT development in these regions. I describe the divergent perceptions of the regulatory space and the contrasting perceptions of the role of private actors in cyber governance. Building on these insights, I argue that there is a conceptual misalignment between Russian and Western approaches in terms of the legal object of regulation and its scope, as well as in the governance models applied in the ICT domain. These differing conceptions contribute to conflicting institutional and normative approaches to international law.

Keywords

Cybersecurity, Information Security, Russia, Cyber Sovereignty, Multistakeholderism

Author Information

Liliya Khasanova is a post-doctoral research fellow with the Berlin-Potsdam Research Group: "The International Rule of Law - Rise or Decline?" in Berlin, Germany. Email: liliya.khasanova@kfg-intlaw.de

Table of Contents

Introduction

The rapid development of ICTs has opened up a new dimension in international law and international relations that has posed a number of intricate technical, conceptual, evidentiary, and legal challenges. Given the growing interdependence, transitioning of economies and societies online, the increasing role of non-state actors, and the emerging problems for existing principles of international law, governments are seeking to find working institutional and regulatory solutions to govern the ICT domain. However, understanding and determining the scope of the domain differs significantly across the increasingly contradictory realities of governments worldwide.

ICTs and the internet exhibit several unique features to which general rules of international law, created and developed in the past eighty years, provide minimal convincing answers (Kettemann 2020; Krieger and Nolte 2016). It is uncontested today that international law applies to cyber operations in cyberspace (UNGA 2013), but disagreement still exists on *how* it applies to cyberspace. Mattias Kettemann argues that international law is the only normative order that can deal systematically with the variety of actors relevant to the internet's use and development (Kettemann 2020). Whether it is true or not, the need for regulating the cyber domain comes at a time when the world is increasingly divided, with shifting and elusive power balances (Gao and Chen 2022; D. Broeders and Berg 2020) and strong forces against "Western hegemony" in cyberspace (Zang 2022).

The parallel existence of two forums on cybersecurity under UN auspices—the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG)—perfectly illustrates the cultural opposition in how states view cybersecurity. Russia, which initially proposed the GGE in 2002 with the idea of negotiating an international treaty, decided to pursue an alternative route through another forum that included all UN members. This move was made to restart the discussion on an international treaty after facing strong pushback in the GGE.

Although the last mandate of the GGE was not renewed, the confrontation persists as the Program of Action (PoA) - a proposal initiated by France and Egypt in 2020 - introduced an alternative to the OEWG negotiation format ("Programme of Action Proposal" 2020). Observation of the various international negotiation forums in cybersecurity shows that parties involved do not have the same understanding of what and how they are seeking to regulate, which constitutes one of the major obstacles to successful discussions. In fact, it is analytically unhelpful to assume there is a common understanding of the scope and goals of international regulation in the ICT field. Reaching an agreement in the absence of a basic understanding of each other's doctrines might result in incomprehensive agreements, difficulties in implementation and escalation of conflicts (Giles and Hagestad 2013). I build on the idea that there are many approaches to ICT governance and those are not necessarily the same around the world.

Russia and Western countries have persistently used different language related to the ICT '*space*'. It has been understudied that Russia is constantly referring to 'information space', while Western countries use the term 'cyberspace'. Hence, given the lack of understanding of each other's doctrines and ideas behind concepts, I start from the very beginning and analyze whether 'information space' in Russian understanding is the same as 'cyberspace' in Western understanding. If not, what are the core differences in ideas behind those concepts and how do they influence the states' approaches to international regulation of cyber operations?

To answer these questions, I conduct a comparative legal analysis with a particular focus on sources of international law, national legislations in Russia and Western countries, international cyber governance documents and normative proposals from States. However, recognizing that laws exist in a historical, social and political context, I also draw on differences in the evolution of the ICT and internet landscape, official statements of state representatives (both in international and national settings), discourses dominating in the governing elites and academia and state practice.

I start with a discussion on how we should think about notions of 'interests - conceptions - approach' in a comparative setting and contextualise the Western and Russian approaches among several others. The next part focuses on two identified key areas of conceptual discrepancies between the Russian and Western approaches to cyberspace: (a) the misalignment of the scope between 'information space and 'cyberspace', which reflects an empirical multiplicity of ideas, interests, regulations and practices, and (b) the differing perspectives on the role of non-state stakeholders in cyber governance. I conclude by outlining both conceptual divergences and slight convergences between the two approaches.

Analytical Framework

This work contributes to the examination of non-western narratives in cybersecurity and builds upon several other studies conducted on Russian information space by Russian and Western legal and political scholars in recent years (Sayapin 2021; Danelyan and Gulyaeva 2020; Pigman 2019; Savelyev 2016; Giles 2012). While views of Russia in international cyber negotiations were explored by scholars, the comprehensive analysis of the Russian concept of ‘information space’ and its influence on the Russian approach to the international law of cyber security (and international law in general) did not receive proper attention. The Russian approach to cyberspace was evaluated by Sergey Sayapin, who conducted a classical legal analysis of relevant legal acts regulating various practices in the ICT field (Sayapin 2021). I am taking a different holistic approach to go beyond positions and laws, looking for interests that form conceptions of information space and which, in turn, form the Russian approach in international law regulating ICTs as compared to Western countries.

Analytically, this paper assesses the Russian approach in comparison to the Western approach, which helps to define both conceptions further, explaining core differences and potential space for convergence. Two points are important to mention in this regard.

Firstly, by Western approach, I mean the shared vision of the application of international law to international cyber security followed by the US, EU and other ‘like-minded states’ in cyber negotiation fora.

Secondly, I acknowledge an empirical multiplicity of approaches to cyber security among Western countries. For instance, in the past decade, following the Snowden revelations, the EU and other players within the Western camp have been seeking strategic autonomy from the US in cyberspace, competing for the global regulator roles (Gao and Chen 2022; Greenleaf 2021) and adopting progressive legislation aimed at defending their economic and national interests that do not necessarily go along with the US vision of open and self-regulated internet. Taking one step further, even within the EU, national positions on how rules of international law apply to cyberspace seem to be varying (Roguski 2020). However, for the comparative analysis on a meta-level that this paper attempts to conduct, the group of ‘Western’ states is sufficient as they share common values of liberal democracy and an understanding of the scope of the cyberspace domain. Although foreign policy interests vary, there is a shared understanding of the scope of the domain and a relatively consonant view on the application of international law. I also consider discrepancies within the Western group of countries where it is relevant.

Thirdly, this paper has a slight emphasis on exploring the Russian approach through international normative initiatives and national legislation, because the Western approach has received extensive coverage in academic research and policy discussion in English. In contrast, as mentioned earlier, the Russian approach has been comparatively less explored and is often less understood by Western audiences. While the Western perspective is included in the paper, its role is primarily to serve as a reference point for comparative analysis and to highlight the distinctions between the two approaches.

It is also important to note that while recognizing certain shared practices and ideas between Russian and Chinese approaches to information space and security, I consider those approaches as distinct. Although piled into one Sino-Russian approach to cyber security by some scholars, Russia and China, despite sharing several common perspectives on cyber governance, have strong institutional and interest divergences when it comes to their national information security (Khasanova and Tai 2023). I do refer to China and other emerging powers in the cyber domain, however, where appropriate and where it helps to explain better the Russian-Western dichotomy.

Acknowledging a deadlock in multilateral cyber negotiations (Duroy and Khasanova 2023) and a strong misalignment in understanding how international law applies to operations in cyberspace, I use one of the main strategies described in negotiation theory. It suggests that in order to identify the zone of possible agreement and resolve conflicts, we need to explore underlying interests behind (state') positions (Fisher, Ury, and Patton 1997; Lewicki, Barry, and Saunders 2020). State interests can be influenced by various factors and defined by a range of actors. State interests directly inform 'conceptions' or 'understanding'. In other words, understanding/conception is rooted in the interests of a particular government at a particular time. Examining these underlying logics is important for the exploration of different approaches with a further goal of the potential reconciliation of shared interests.

Therefore, in this paper, I examine the conceptual differences between purportedly divergent approaches to international law and governance by starting to look at two core overarching concepts: cyber-space (-security) and information space (-security). To this end, I will investigate the linguistic terminology, the meaning of such terms as found in policy and legal documents and the implications of such policies, laws and ideas in state practice. I am also looking at different conceptions of internet governance or public-private relationship seeking to define the scope of the concepts further.

Conceptual Differences

This section delineates two key distinctions between the two approaches to cyberspace regulation. The first distinction pertains to the use of differing terminologies for referring to the concepts of 'information space' and 'cyberspace'. The second distinction revolves around divergent perspectives on the role of private actors in cyber governance.

Defining the 'Space': Russian 'Information Space' and its Difference from 'Cyberspace'

The difference in terminology between Russian and Western narratives in regulating the ICT 'space' is neglected both in theoretical understanding and practical implementation. Meanwhile, negotiation theory emphasizes the importance of defining the scope of the negotiation as a fundamental initial step (Fisher, Ury, and Patton 1997; Lewicki, Barry, and Saunders 2020).

Information space (and security) are terms used both by Russia and China in all international deliberations related to the ICTs. Some differences between the Russian and Chinese concepts were briefly identified, with the former's vision including human information processing and the latter's center on global information and communications network (Giles and Hagestad 2013). One does not need to be a linguist to sense the difference between the terms 'information space (security)' and 'cyberspace (security)'. The literal reading suggests that the first space encompasses everything related to the production, use, impact, exchange of information, while the scope of the second one is limited by 'cyber', which usually refers to physical infrastructure (computers, internet-enabled devices, servers, routers, and other components), logistical world and the virtual world (Oxford Reference 2023). In other words, the term 'information space' is broader and encompasses 'cyberspace' plus information management.

What is information space and information security in Russian understanding and how is it different from cyberspace and cyber security used by Western countries? To empirically assess this 'space', I will first analyse the definitions of information space contained in Russian normative and policy documents, both national and international and will compare it against the definitions of cyberspace. Secondly, I will outline the state practice on information space and security in Russia that illustrates the conception further.

Characteristics of 'Information Space'

In normative and policy documents adopted by Russia nationally and proposed internationally, there is no set definition of information space and security. Rather, there are several fluctuating definitions depending on the type of document. Nevertheless, important characteristics of the information space can be traced across all the documents.

Firstly, all definitions of 'information space' or 'information sphere' include information or information resources in the object of legal regulation. Back in 1995, the 'Concept of Formation and Development of the Russian Information Space and Related State Information Resources' stipulated the following main components of information space: information resources (data and knowledge) and information infrastructure (organizational and technical structures) (Russian Government 1995). The latest Doctrine of Information Security (2016) provides the following definition of the 'information sphere':

> "...combination of information, informatisation objects, information systems and websites within the internet, communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere".

Therefore, information itself is a part of the object of legal regulation along with information infrastructure. A similar logic can be found in international documents proposed by Russia under UN auspices. Russia's Draft Convention on International Information Security (2011), also defines the concept of 'information space' by considering information as an essential component of that space.[1]

The term cyberspace ('киберпространство') is rare in Russian documents and statements and appears mostly when referring to the 'Western' approach. The Western definition of cyberspace predominantly started with an understanding that it is a virtual environment formed by physical and non-physical components that store, modify and exchange data using computer networks (Schmitt 2017, 564). This was the definition agreed upon in the Tallinn

[1] Note: Information space is defined as 'the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself'.

Manual 2.0, which in 2017 represented the views of several, predominantly Western, international scholars. Similar interpretations can be found in various country statements regarding the application of international law in cyberspace.[2]

Secondly, information security language closely relates to the cognitive implications of information on society. Contrary to Western approaches, the Russian government views both the mind and information systems as integral parts of its concept of information security(Thomas 2001). When looking at the scope of the information space, Russian scholars rely on a broad overarching concept quoting the Okinawa Charter on Global Information Society (2000) that notes the 'revolutionary impact of the information that affects the way people live, learn and work…' ("Okinawa Charter on Global Information Society" 2000) or UNESCO reports that stipulate that 'the information sphere is a sphere of conscious life, from education to science, from culture to communication'(Ivanov 2005).

These sociological, and cultural dimensions of information play an integral part in defining 'information space' and information security challenges. The capacity of information flows to affect individual and social consciousness is a concern and one of the main underlying logics in most of the Russian national documents and international statements or proposals. Protection of Russian society from the 'destructive information and psychological impact' is a national security concern (Russian Government 2021).

This leads to the third explicit characteristic that characterizes the Russian concept of information space and security: the perception of the information space as a source of constant security challenges to individuals, society and the state.

Russian normative proposals and legal academic literature in the 1990s perceived information space as a global domain that facilitates international communication, and the limitation of information flows as a violation of the right to information (Russian Government 1995; Ivanov 2005). However, it did not take long for the 'territorialization' of information space with a traditional vision of sovereign states' rights in this common sphere. The Snowden revelations in 2013, colour revolutions in Ukraine and Georgia, regime changes in the Middle East, and Putin's return to presidency became a fertile ground for Russian political elites to build their perceptions on information threats to regime security that firmly integrated into broader national security narratives (Pigman 2019). The threat to political, economic and social stability by information that is manipulated and imposed on internet users has been outlined in multiple official documents. For example, the Doctrine of Information Security (2016) elaborated on the national interests of Russia including the 'protection of an individual, society and the state against internal and external information threats, allowing to ensure…the sovereignty, the territorial integrity and sustainable socio-economic development'. Additionally, the National

[2] Note: For example, the German Position Paper on the Application of International Law in Cyberspace defines cyberspace as "the conglomerate of (at least partly interconnected) 'cyber infrastructures' and 'cyber processes'", where cyber processes are 'events and sequences of events of data creation, storage, processing, alteration or relocation through means of information technology' (German Federal Foreign Office 2021); Same logic follows the French statement, focusing mainly on malicious cyber operations that target government and administration information systems (Ministry of Defense, France 2021).

Security Strategy (2021) warns against the imposition of a ‘distorted view of historical facts and events in Russia and abroad’.

The same rhetoric and logic were reflected in international normative proposals. The International Convention on Information Security (2011) adopted strong sovereignty language recognizing political independence and territorial integrity of states. The Code of Conduct (2015) calls for ‘respect for diversity of history, culture and social systems of all countries’. Arguments on the perseverance of societal norms and historic justice are strong, representing a continuation of civilizational identity claims and ‘civilizational otherness’(Mälksoo 2015) of Russia being enacted in cyber narratives as well.

In Western cybersecurity narratives, the power and threat of information operations and activities are also increasingly recognized. There is a growing realization that other states and non-state actors are capable of manipulating information or conducting online activities to change or reinforce the attitudes or behaviours of the targeted audience. However, those narratives are mostly at the periphery or even outside of the international cyberspace/cybersecurity debate which mostly focuses on the protection of ICT infrastructure, free data flows, freedom of information and other digital rights. Although the sense of fragmentation of international cyber governance is growing (Segal 2022), along with the development of digital sovereignty narratives in liberal democracies (Dennis Broeders et al. 2022), in the eyes of the West, the internet is a global domain with its predominantly ‘technical’ security challenges. Meanwhile, in Russian understanding, beside technical cybersecurity challenges, the state is responsible for ‘security’ information which ultimately secures its national sovereignty and civilizational values.

Translating Conceptions into State Practice

Russian perception of information space and security is reflected in recent policies that regulate the security of information infrastructure (software or hardware) and information itself. Several waves of legal developments and amendments to existing laws have led to systemic changes and the expansion of institutional powers in controlling information content and movement. Ironically, the official rationale to protect ‘individuals, society and the state against international and external information threats’ (which is repeated in all Russian documents related to information security) has resulted in an overarching control over networks and minds. Joining the parade against US hegemony in cyberspace (Zang 2022), Russia went further by establishing a digital sovereignty doctrine with all its implications.

This paper groups several of the milestones in translating the official rhetoric of information space into state practice relevant to the characterization of the ‘space’.

The first key pieces of legislation were characterized by the intention of gaining control over information and its dissemination. In 2014, a set of amendments were adopted to Federal Law No.149-FZ “On Information, Information Technologies and Protection of Information” that introduced the concept of the ‘organiser of dissemination of information in the internet referring to providers of ‘communication internet-services’ operating in Russia (Russian Government 2014a; Savelyev 2016). Such internet service providers had to register with the Federal Service for Supervision of Communications, Information Technology and Mass Media (hereinafter - "Roskomnadzor"), store a copy of the user's traffic and several types of data in Russia and cooperate with the Federal Security Service (FSS). Subsequent legislation introduced amendments requiring all personal data operators to record, store and process any personal data of Russian individuals in databases located in Russia as a primary step (Russian Government 2014b). These changes forced companies to resort to third-party data centers located in Russia within one year of the law's passage. According to the head of Roskomnadzor, at least 600 foreign companies sent notifications on moving their data processing and storage to Russian territory (RBC 2021). On the institutional side, Roskomnadzor received extensive authority in controlling and enforcing compliance by conducting scheduled or unscheduled audits related to data privacy protection, managing 'black lists' of companies that do not comply with requirements of data protection or localization, initiating legal actions in court, and restricting access to certain websites. Since 2016, big international companies (mostly social media companies) have been held liable for violating data localization requirements (e.g. Facebook, Twitter, Google) or have been blocked on the territory of Russia (e.g. LinkedIn).

The second cluster of developments in Russian law targeted strategic autonomy in a technological sense. In 2019, the Sovereign internet Law aimed at the independent functioning of the Russian segment of the internet was adopted (Russian Government 2019), fulfilling the aspirations for establishing a Runet as earlier described in the Information Security Doctrine (2016) (Russian Government 2016) and the Information Society Development Strategy for 2017 – 2030 (President of the Russian Federation 2017). The officially declared aim of the Runet is the protection of the Russian segment of the internet and its uninterrupted functioning against external threats. The 2017 Law on Security of Information Infrastructure (Russian Government 2017), prescribed the transfer of all security infrastructures to primarily Russian software and hardware, which is planned to be completed by 2025.

Finally, justification of censorship in the name of national sovereignty was reinforced in 2020 in relation to the 'unauthorized public protests', establishing an administrative liability for failure to comply with the requirements for providers to restrict access to information that is considered illegal in Russia (Russian Government 2020). Blocking websites because of their illegal content became a norm and reached its culmination in 2022 with the criminalization of public dissemination of 'knowingly false information' about Russian armed forces in relation to the conflict in Ukraine, known as the law on 'fakes' (Russian Government 2022). According to a the Freedom House, as of August 2022, seventy-five criminal cases were initiated in Russian courts under article 207.3 of the criminal code (on public dissemination of knowingly false information), with fourteen individuals found guilty (Freedom House 2022). Notably, the persecution is always done in the name of the laws which are amended and adopted in very short timeframes, confirming the long-standing tradition of the 'rule *by* law'.

To summarize, the definitions found in law and state practice prove that the Russian understanding of the concept of information space extends beyond the boundaries of cyberspace. It encompasses not only material and non-material technical aspects of cyberspace but also information itself along with its cognitive implications for society. The short period of relative freedom experienced in the 1990s rolled back to long-standing historical traditions of state control and a mindset focused on external geopolitical threats. Russian policymakers and scholars have conveniently applied and adapted the long-standing concept of sovereignty in its traditional Westphalian sense to the realm of cyberspace, intending to challenge the Western principles of internet and information freedom. The implementation of infrastructural barriers, the shutdown of independent media, and the use of application-level blocking contribute to the establishment of the Russian information iron curtain. This vision is firmly rooted in alleged sovereign national security interests and will have far-reaching implications for Russian society, international law and international relations.

Governing the 'Space': the Role of Non-Governmental Actors

The technical reality of cyberspace underscored the role private actors and non-governmental organizations play in filling the technical and policy gaps in internet governance. Empirically, the public-private dichotomy varies depending on the policy area. Three decades ago, states had a limited role in internet governance, especially in the Western world(Barlow 2019). However, the idea of a self-governing global network is now a utopia, as governments gradually increase their regulation of the internet. The current ecosystem of internet governance is sustained both by state and non-state actors, although the decision-making and norm-making space of non-state actors in some regions is rapidly shrinking.

The conference of the International Telecommunication Union in 2012 disclosed differences in global internet governance approaches (ITU 2012). Russia, among other countries, pushed for a state-centric approach in a traditional multilateral sense, while Western countries led by the U.S. endorsed a multi-stakeholder approach (Fidler 2013).

In international settings, Russia has advocated for the multilateral approach whereby 'states play the main role and bear equal responsibility in international internet governance'(Permanent Mission of the Russian Federation to the United Nations 2022). The traditional feature associated with the Russian doctrine of international law perceives the state as the main subject of international law (Mälksoo 2015) and legal norms only as the result of the state will echo vividly in international, regional, and national normative cyber proposals and statements across institutions in the ICT field. Hence, the categorical rejection of individual and transnational corporations (TNC) as subjects of international law plays out equally in cyberspace rhetoric.

Under UN auspices, Russian proposals such as the International Code of Conduct for Information Security (2015) or the Draft Convention on Cooperation in Combating Information Crimes (2021) affirm visions of state-centrism and sovereignty in the information space. In OEWG negotiations, Russia gradually pushes back on strong multi-stakeholder provisions, noting that '...the role of a multistakeholder approach to ensuring international information security is exaggerated by imposing the idea that States and other stakeholders hold similar responsibility in this area' (Russian Ministry of Foreign Affairs 2021). In addition, deepening cleavages between Western states and Russia heavily influence the participation of certain stakeholders in the OEWG meetings. For example, in July 2022 twenty-two international NGOs and several Russian organizations had their accreditation blocked by Russia and Ukraine (Duroy and Khasanova 2023).

In regional settings, agreements on information security within the framework of the Shanghai Cooperation Organization (SCO) and joint statements of Russia and China follow the same rhetoric on the primary role of states in internet governance ("Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development" 2022). The private ICT sector in Russia is highly regulated and controlled by the government. Meanwhile, foreign tech giants are facing fines or expulsion from the Russian market if they do not comply with national requirements. For example, strict data localization laws and rules on content control were enforced extensively in 2022 (Khasanova and Tai 2023; Anyukhina 2022).

The current approaches to internet governance can be better understood by examining the historical development of the internet landscape in the region. For the Soviet Union, the employment of computer systems and nationwide networks primarily served to maintain existing economic and political order rather than promote reform, contrary to the anticipation of the Soviet scientists (Gerovitch 2008). The Soviet legal scholarship supported 'statism' in international information space, claiming the state's margin of appreciation to limit the type of information that goes contrary to its Constitution (Grohal'ski, 1984; Shevcova 1981). Despite a brief period in the 1990s when attention was given to the internet's economic potential and Russia's integration into the global information space, network governance has consistently been heavily centralized, even in the presence of a fragmented infrastructure of internet service providers. The Russian government currently does not just set the main regulations in the field, but also has direct access to boards of directors and the internal functioning of major tech companies (Glasze et al. 2022). The absence of national tech giants that developed independently and the lack of effective consulting procedures reflects the historically centralized, top-down internet governance model in Russia (Khasanova and Tai 2023).

By paying close attention to statements of Russian representatives at the negotiation forums and analyzing the government's proposals in pursuing the 'sovereign internet' idea, one can conclude the Russian government pursues autonomy in information space and independence from foreign technological giants. More specifically, autonomy in both a technological and information content sense follows the 'information space' logic. The National Security Strategy (2021) speaks critically about TNCs that have 'monopolized' control over internet information resources and are practicing censorship and manipulation of information *contrary to the rules of international law* [emphasis added] (Russian Government 2021).

Finally, it should be noted that in the Russian government's understanding, a state-centric approach does not mean there is no place for private actors. It means that the authority and decision-making powers are attributes of a state, while private actors play a subsidiary role.

In contrast, Western like-minded states endorse a multi-stakeholder approach in internet governance where shared principles, norms, rules, decision-making procedures and programmes are developed and applied by governments, the private sector, and civil society. Following this approach, private companies, non-governmental organizations, and civil society play a significant role in the evolution (Tsagourias 2017) and implementation (Kumar 2021) of cyber norms by providing recommendations and feedback. One of the main rationales behind the Program of Action proposal initiated by France and Egypt in 2020 was the meaningful inclusion of various stakeholders in negotiations and the expansion of space for sharing practices ("Programme of Action Proposal" 2020).

From a historical perspective, the Western internet landscape evolved in a highly decentralized manner. The interaction between states and non-state actors initially was defined by technical coordination, due to the academic freedom granted to researchers developing the network and then the impossibility of controlling the burgeoning internet initiatives (Radu 2019). Three decades ago, some scholars insisted that states were just among other stakeholders and that cyberspace should be a self-regulated environment (Johnson and Post 1996; Barlow 2019). The situation nowadays is drastically changing as States increasingly claim the regulatory space with normative efforts aimed at controlling tech giants. The EU Digital Services Act (European Parliament 2022b) and Digital Markets Act (European Parliament 2022a) are perfect examples of attempts to regulate the 'Wild West' by protecting the fundamental rights of users and local tech markets from monopolization. In the US, the public-private equilibrium takes a different turn with the extremely powerful private sector that sets many standards in the absence of comprehensive federal regulation, the constitutional First Amendment that protects freedom of speech and the absence of federal privacy law, while constitutional protections and state laws shape the boundaries of privacy and free speech. For example, in the case of content moderation, there is an emergence of models of privately driven transnational hybrid adjudication (Gulati 2022). Meanwhile, States of Texas and Florida separately adopted legislation restricting content moderation by social media platforms. They were eventually appealed, but the two US Courts of Appeal have taken different positions (the Texas law stayed in force, and the Florida one was blocked), leading the matter to the US Supreme Court (Congressional Research Service 2022).

Thus, considering the history and influence of the Western TNC in cyberspace, this public-private cooperation is inevitable. By maintaining the multi-stakeholder approach, the US handles partnerships with an influential and knowledge-containing private sector, while the EU focuses on the promotion of its values by actively involving civil society in negotiations.

To summarize, the Russian top-down, state-centric approach with a subsidiary role of non-state actors is a combination of historical developments in the ICT field and the Russian traditional 'statist' philosophy of international law. The desire to counterbalance a monopoly of foreign tech giants and to maintain technological independence is coupled with authority over the information domain to ensure the security of the regime. Therefore, while Western cyberspace is a multiplicity of state, non-state and civil society actors, information space in Russian understanding is dominated by states as any other field of classical international law.

Most of the GGe and OEWG consensus reports under UN auspices include references to the multi-stakeholder approach. In practice, multistakeholderism is a reality. For example, in 2022 the OEWG introduced modalities for the participation of stakeholders (OEWG Chair 2022), and the ongoing negotiations on the cybercrime convention include the highest number of stakeholders actively participating in deliberations (Pavlova and Lindsey (Curtet) 2023). Despite different ideas behind the involvement of non-state actors in cyber governance, there is a shared understanding that the final decision-making power is vested in states. In fact, the poles that were once extreme are coming closer: there is a genuine understanding of the role of private actors from the state-centric Russia and a noticeable effort from Western countries to manage the economic and societal impact of the big tech and decentralized finance initiatives.

In actuality, the choice between the two approaches is not binary; rather, the distinction lies in the extent of authority assigned to the private sector. This discrepancy is further reflected in Russia's stance on the role of soft law in governing the information space. The misalignment comes down to competing perspectives of pluralist minimalism with a traditional emphasis on sovereignty and the pursuit of a more ambitious set of institutions and practices.

Conclusion

The differences between Russian 'information space' and Western 'cyberspace' is not merely a matter of terminology, but rather a deeper conceptual divergence in understanding the domain which the two sides are aiming to regulate. The Russian understanding of information space encompasses not only technical aspects of it but also information itself with all its cognitive implications for society. Additionally, the decision-making in information space is vested primarily in sovereign states. Conversely, the Western perspective perceives cyberspace and security from a more technical side, promoting freedom of information and leaving more regulatory space for the private sector and non-state actors. Based on these insights, I conclude that there is a conceptual misalignment between Russian and Western approaches in terms of the legal object of the regulation and its scope, as well as in governance models of the ICT domain. These divergent conceptions inform conflicting approaches to international law in the institutional and normative sense.

The Russian and Western governments are pursuing different sets of interests and goals in their respective 'spaces', and it is a difficult task to trace similarities in understanding international law unless any parts of these conceptions overlap. Therefore, the initial step is to recognize that the parties perceive the domain in different ways to avoid counterproductive discussions and agreements that are difficult to implement.

The presence of different approaches does not mean there is no place to deal with such empirical multiplicity by finding shared interests. State practice signals some shifts: there is a certain re-evaluation by Western countries of the critical role that information plays in socio-political life and an exploration of content management techniques, keeping fundamental rights in mind. On a governance level, the Russian government cannot deny the role that private actors play in space, while the concept of 'digital sovereignty' gains prominence in Western discourse as means of managing the economic and societal impact of large technology corporations.

This finding invites further reflection on the heterogeneity of approaches to cyber/information governance and underscores the importance of addressing these divergences to create more effective and sustainable regulatory frameworks. The failure of past attempts to create universal systems by ignoring conceptual differences demonstrates the need for greater awareness and understanding of the digital domain's complexity.

References

Anyukhina, Irina. 2022. “Russia - Data Protection Overview.” https://www.dataguidance.com/notes/russia-data-protection-overview-0.

Barlow, John Perry. 2019. “A Declaration of the Independence of Cyberspace, Duke Law & Technology Review.” *Duke Law & Technology Review* 18: 5–7.

Broeders, D., and Bibi van den Berg, eds. 2020. *Governing Cyberspace: Behavior, Power, and Diplomacy*. Digital Technologies and Global Politics. Lanham: Rowman & Littlefield.

Broeders, Dennis, Raluca Csernatoni, Kristina Irion, Monica Kaminska, Giorgio Monti, Margarita Robles-Carrillo, Simona Soare, and Paul Timmers. 2022. “Digital Sovereignty: From Narrative To Policy?” https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/_dpBkAW4/digital-sovereignty-from-narrative-to-policy.pdf.

Congressional Research Service. 2022. “Free Speech Challenges to Florida and Texas Social Media Laws.” https://crsreports.congress.gov/product/pdf/LSB/LSB10748.

Danelyan, A. A., and E. E. Gulyaeva. 2020. “International Legal Aspects of Cybersecurity.” *Moscow Journal of International Law*, no. 1 (July): 44–53. https://doi.org/10.24833/0869-0049-2020-1-44-53.

Duroy, Sophie, and Liliya Khasanova. 2023. “Cyberespionage and Human Rights: A Dissapointing Balance.” In *The Challenge of Global Cybersecurity*.

European Parliament. 2022a. *Regulation (EU) 2022/1925 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925.

———. 2022b. *Regulation (EU) 2022/2065 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)*.

Fidler, David. 2013. “internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations | ASIL.” February 7, 2013. https://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision.

Fisher, Roger, William Ury, and Bruce Patton. 1997. *Getting to Yes: Negotiating an Agreement without Giving In*. 2nd ed. London: Arrow Business Books.

Freedom House. 2022. “Russia: Freedom on the Net 2022 Country Report.” Freedom House. https://freedomhouse.org/country/russia/freedom-net/2022.

Gao, Xinchuchu, and Xuechen Chen. 2022. “Role Enactment and the Contestation of Global Cybersecurity Governance.” *Defence Studies* 22 (4): 689–708. https://doi.org/10.1080/14702436.2022.2110485.

German Federal Foreign Office. 2021. “On the Application of International Law in Cyberspace.”

Gerovitch, Slava. 2008. “InterNyet: Why the Soviet Union Did Not Build a Nationwide Computer Network.” *History and Technology* 24 (4): 335–50. https://doi.org/10.1080/07341510802044736.

Giles, Keir. 2012. “Russia’s Public Stance on Cyberspace Issues.” In *NATO CCD COE Publications, Tallinn*.

Giles, Keir, and W. Hagestad. 2013. “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English.” In *Cyber Conflict (CyCon), 2013*, 1–17.

Glasze, Georg, Amaël Cattaruzza, Frédérick Douzet, Finn Dammann, Marie-Gabrielle Bertran, Clotilde Bômont, Matthias Braun, et al. 2022. "Contested Spatialities of Digital Sovereignty." *Geopolitics* 0 (0): 1–40. https://doi.org/10.1080/14650045.2022.2050070.

Greenleaf, Graham. 2021. "The 'Brussels Effect' of the EU's 'AI Act' on Data Privacy Outside Europe." SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=3898904.

Grohal'ski, Stefan-Marek. 1984. "Svobodnoe Dvizhenie Informacii i Mezhdunarodnoe Pravo." https://www.dissercat.com/content/svobodnoe-dvizhenie-informatsii-i-mezhdunarodnoe-pravo.

Gulati, Rishi. 2022. "KFG Working Paper Series," no. No. 53 (March).

Ivanov, A.K. 2005. "Global'noe Informacionnoe Prostranstvo i Ego Mesto v Sovremennom Mezhdunarodnom Prave," no. 1: 219–29.

ITU. 2012. "New Global Telecoms Treaty Agreed in Dubai." https://www.itu.int/net/pressoffice/press_releases/2012/92.aspx.

Johnson, David R., and David Post. 1996. "Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review* 48 (5): 1367. https://doi.org/10.2307/1229390.

"Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development." 2022, February 4, 2022. http://en.kremlin.ru/supplement/5770.

Kettemann, Matthias C. 2020. "The Normative Order of the internet." In *The Normative Order of the internet: A Theory of Rule and Regulation Online*, edited by Matthias C. Kettemann, 0. Oxford University Press. https://doi.org/10.1093/oso/9780198865995.003.0006.

Khasanova, Liliya, and Katharin Tai. 2023. "An Athoritarian Approach to Digital Sovereignty? Russian and Chinese Data Localization Models."

Krieger, Heike, and Georg Nolte. 2016. "The International Rule of Law - Rise or Decline? Points of Departure." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2866940.

Kumar, Sheetal. 2021. "The Missing Piece in Human-Centric Approaches to Cybernorms Implementation: The Role of Civil Society." *Journal of Cyber Policy* 6 (3): 375–93. https://doi.org/10.1080/23738871.2021.1909090.

Mälksoo, Lauri. 2015. *Russian Approaches to International Law*. Oxford University Press.

Ministry of Defense, France. 2021. "International Law Applied to Operations in Cyberspace."

OEWG Chair. 2022. "Open-Ended Working Group on Information and Communication Technologies (2021) | United Nations (Unoda.Org)," April 22, 2022. https://documents.unoda.org/wp-content/uploads/2022/04/Letter-from-OEWG-Chair-22-April-2022.pdf.

"Okinawa Charter on Global Information Society." 2000. Ministry of Foreign Affairs of Japan. https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html.

Pavlova, Pavlina, and Charlotte Lindsey (Curtet). 2023. "A Year of United Nations Cybercrime Negotiations." *CyberPeace Institute* (blog). February 28, 2023. https://cyberpeaceinstitute.org/news/a-year-of-united-nations-cybercrime-negotiations-the-message-of-the-multi-stakeholder-manifesto-remains-central-as-the-process-moves-forward/.

Permanent Mission of the Russian Federation to the United Nations. 2022. "Statement by Head of The Russian Interagency Delegation to the First Substantive Session of The UN Open-Ended Working Group on Security of And in The Use of ICTs 2021-2025, Deputy Director of The Department of International Information Security of The Ministry of

Foreign Affairs of The Russian Federation Dr Vladimir Shin." https://estatements.unmeetings.org/estatements/12.1255/20220330/zQAu2Wo0dGU9/rfmky7X1Pa1G_en.pdf.

Pigman, Lincoln. 2019. "Russia's Vision of Cyberspace: A Danger to Regime Security, Public Safety, and Societal Norms and Cohesion." *Journal of Cyber Policy* 4 (1): 22–34. https://doi.org/10.1080/23738871.2018.1546884.

President of the Russian Federation. 2017. "*O Strategii razvitija informacionnogo obshhestva v Rossijskoj Federacii na 2017 – 2030 gody".* http://kremlin.ru/acts/bank/41919.

"Programme of Action Proposal." 2020. https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.

Radu, Roxana. 2019. *Negotiating Internet Governance*. First edition. Oxford, United Kingdom ; New York, NY: Oxford University Press.

RBC. 2021. "Vlasti Napravili Inostrannym Kompanijam Zaprosy o Hranenii Dannyh Rossijan," June 29, 2021. https://www.rbc.ru/technology_and_media/28/06/2021/60d6d5cb9a7947e0a57257a2.

Roguski, Przemysław. 2020. "Application of International Law to Cyber Operations: A Comparative Analysis of States' Views." *The Hague Program for Cyber Norms Brief*, 52.

Russian Government. 1995. "Koncepcija Formirovanija i Razvitija Edinogo Informacionnogo Prostranstva Rossii i Sootvetstvujushhih Gosudarstvennyh Informacionnyh Resursov." November 23, 1995. https://rulaws.ru/acts/Kontseptsiya-formirovaniya-i-razvitiya-edinogo-informatsionnogo-prostranstva-Rossii-i-sootvetstvuyuschih-gosu/.

———. 2014a. *Federal Law No.97-FZ "On Amendments to the Federal Statute 'On Information, Information Technologies and on the Protection of Information' and Specific Legal Acts of the Russian Federation on the Issues of Regulation of Information Exchange with the Use of Telecommunication Networks."*

———. 2014b. *Federal Law No. 242-FZ On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks*.

———. 2016. *Doctrine of Information Security of the Russian Federation December 2016 | Public Intelligence. https://publicintelligence.net/ru-information-security-2016/.*

———. 2017. *Federal Law No. 187-FZ On the Security of Critical Information Infrastructure of the Russian Federation*.

———. 2019. *Federal Law No. 90- FZ On Introducing Amendments to the Federal Law on Communications and the Federal Law On Information, Information Technologies and Protection of Information Dated*.

———. 2020. *Federal Law No. 511-FZ On Introducing Amendments to the Russian Federation Code of Administrative Offences*.

———. 2021. "'Strategiia Natsionalnoi Bezopasnosti Rossiiskoi Federatsii.'" http://publication.pravo.gov.ru/Document/View/0001202107030001.

———. 2022. *Federal Law No. 32 – FZ On Introducing Amendments to the Criminal Code of Russian Federation and Articles 21 and 151 of Criminal Code of Procedures of the Russian Federation.*

Russian Ministry of Foreign Affairs. 2021. "Commentary Of The Russian Federation On The Zero Draft Report Of The Open-Ended Working Group On Developments In The Field Of Information And Telecommunications In The Context Of International Security."

Savelyev, Alexander. 2016. “Russia’s New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction?” *Computer Law & Security Review* 32 (1): 128–45. https://doi.org/10.1016/j.clsr.2015.12.003.

Sayapin, Sergey. 2021. “Russian Approaches to International Law and Cyberspace.” In *Research Handbook on International Law and Cyberspace*, 2nd ed., 22. Edward Elgar Publishing.

Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. 2nd ed. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524.

Segal, Adam. 2022. “From Defending the Open Internet to Confronting the Reality of a Fragmented Cyberspace: Reflecting Upon Two CFR Reports on U.S. Goals in Cyberspace.” *Lawfare* (blog). August 11, 2022. https://www.lawfareblog.com/defending-open-internet-confronting-reality-fragmented-cyberspace-reflecting-upon-two-cfr-reports-us.

Shevcova, Svetlana. 1981. “Ispol’zovanie Sredstv Massovoj Informacii v Svete Principa Gosudarstvennogo Suvereniteta.”

Thomas, Timothy L. 2001. “Information Security Thinking: A Comparison of U.S., Russian, and Chinese Concepts.” APAN Community. August 1, 2001. https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/240293.

Tsagourias, Nicholas. 2017. “The Rule of Law in Cyberspace: A Hybrid and Networked Concept?,” 20.

UNGA. 2013. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” A/68/98. https://undocs.org/A/68/98.

Zang, Dongsheng. 2022. “Revolt against the U.S. Hegemony: Judicial Divergence in Cyberspace” 39 (1): 71