Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurìdico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

ANTONIO MARICONDA*

SOVEREIGN EQUALITY, NON-INTERFERENCE AND "INFORMATION SECURITY": THE NEW UN CYBERCRIME CONVENTION AS A MIRROR OF THE SINO-RUSSIAN STANCE ON INTERNATIONAL LAW

1. *Introduction*

On 24 December 2024, the UN General Assembly adopted a new Convention on Cybercrime, aimed at "Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes"[1] ("UN Cybercrime Convention" or "Convention"). The Convention is the result of extensive negotiations conducted within the dedicated Intergovernmental Ad Hoc Committee, established by the

* Postdoctoral Research Fellow in International Law, University of Milan.
[1] See UNGA Res 79/243 (24 December 2024) UN Doc A/RES/79/243.

UN General Assembly in 2019 ("AHC")[2], where Russia played a leading role as the principal promoter of the treaty[3] alongside China[4]. The Convention, which will open for signature in October 2025 and enter into force upon the 40th ratification, represents the first globally adopted treaty specifically dedicated to cybercrime[5]. Its structure reflects a comprehensive approach to the issue, encompassing chapters on substantive criminal law, procedural measures, international cooperation, technical assistance, prevention, and mechanisms for implementation[6]. In doing so, it positions itself as a multilateral alternative to existing regional instruments, such as the Budapest Convention adopted by the Council of Europe[7].

While the UN Secretary-General's spokesperson stated that «the treaty is a demonstration of multilateralism succeeding during difficult times and reflects the collective will of Member States to promote international cooperation to prevent and combat cybercrime» [8], and INTERPOL welcomed its adoption[9], some NGOs[10] and scholars[11] have criticized it as an attempt by autocratic regimes to challenge the so-called US-dominated cyber liberal order, shifting away from the multistakeholder model in favor of a State-centric vision of internet governance, characterized by the assertion of absolute national sovereignty over cyberspace[12].

---

[2] See UNGA Res 74/247 (27 December 2019) UN Doc A/RES/74/247. On the sessions of the Committee, see www.unodc.org.

[3] R. IYENGAR, R. GRAMER and A. RATHI, *Russia Is Commandeering the U.N. Cybercrime Treaty*, in *Foreign Policy*, 31 August 2023, available at www.foreignpolicy.com.

[4] A. PETERS, *Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime*, in *Foreign Policy*, 16 September 2019, available at www.foreignpolicy.com.

[5] UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC*), United Nations Convention against cybercrime, Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes - Convention at a glance*, available at www.unodc.org

[6] UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC), *United Nations Convention against cybercrime, Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes – Chapters of the Convention*, available at www.unodc.org.

[7] Council of Europe, Convention on Cybercrime (ETS No. 185), opened for signature on 23/11/2001, Budapest, for the other regional instruments on cybercrime, see UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC), *Sharing Electronic Resources and Laws on Crime (SHERLOC), UNODC Teaching Module Series: Cybercrime – International and Regional Instruments*, available at www.sherloc.unodc.org.

[8] See Statement attributable to the Spokesperson for the Secretary-General - on the adoption of the United Nations Convention against Cybercrime, 24 December 2024, available at www.press.un.org.

[9] *INTERPOL welcomes adoption of UN convention against cybercrime*, 23 December 2024, available at www.interpol.int.

[10] HUMAN RIGHTS WATCH, *New UN Cybercrime Treaty Primed for Abuse. States Should Reject Ratifying Convention on Human Rights Grounds*, 30 December 2024, available at www.hrw.com; see also *Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session*, 23 January 2024, available at www.hrw.com.

[11] T. FALCHETTA, *The Draft UN Cybercrime Treaty Is Overbroad and Falls Short On Human Rights Protection*, in *Just Security*, 22 January 2024, available at www.justsecurity.org; E. SCHER ZAGIER, *The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize,* in *Just Security*, 2 October 2024, available at www.justsecurity.org.; F. SEATZU, *The New UN Convention on Cybercrime: Between Securing Cyberspace and Undermining Fundamental Rights and Freedoms*, in *La Comunità Internazionale*, 2025, p. 227 ss.; S. HARIKRISHNA, *The UN Cybercrime Treaty: A Pandora's Box for Human Rights*, in *Human Rights Research Center*, 6 March 2025, available at www.humanrightsresearchcenter.org.

[12] A. SUKUMAR, A. BASU, *Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order*, in *Journal of Cyber Policy*, 2024, p. 256 ss.; T. GINSBURG, *How Authoritarians Use International Law*, in *Journal of Democracy*, 2020, p. 44 ff.

While much of the debate has focused on the Convention's human rights implications[13], these concerns are only one aspect of its broader significance for international law. The Convention is, indeed, the first binding instrument with a claim to universality where China and Russia have played a dominant role in shaping its content. This influence reflects their shared vision of international law and marks a clear departure from the framework traditionally shaped by Western States. This Sino-Russian dominance was primarily asserted through proposals submitted during the negotiation process, some of which are reflected in the final text.

While China and Russia may not always hold identical views on the international legal order[14], indeed, they undeniably converge on one core principle: the centrality of State sovereignty[15]. This shared position is particularly evident in their Joint Statements on international law, which consistently reaffirm a commitment to three foundational sources: the first is the Mao-era Five Principles of Peaceful Coexistence, which were originally formulated in a 1954 agreement between China and India and reaffirmed the following year at the Bandung Conference. Over time, they came to serve as the ideological backbone of the Non-Aligned Movement and, today, have become a central pillar of contemporary Sino-Russian relations. These principles place mutual respect for sovereignty and territorial integrity at the forefront, followed by mutual non-aggression, non-interference in internal affairs, equality and mutual benefit, and peaceful coexistence[16]. The second reference is to the principles of the United Nations Charter, especially Article 2(1), which affirms the sovereign equality of all Member States and notably places it at the forefront of the Charter's core principles. Complementing these, the third source is the 1970 Declaration on Principles

---

[13] UNITED NATIONS SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF HUMAN RIGHTS WHILE COUNTERING TERRORISM B. SAUL, *Human Rights Assessment of the Draft United Nations Cybercrime Convention*, 25 July 2024, available at www.unodc.org; OFFICE OF THE HIGH COMMISSIONER ON HUMAN RIGHTS (OHCHR), *Human Rights and the Draft Cybercrime Convention*, 2024, available at www.ohchr.org; PRIVACY INTERNATIONAL AND ELECTRONIC FRONTIER FOUNDATION, *Privacy International and Electronic Frontier Foundation's Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty*, 2022, available at www.unodc.org.

[14] For an overview of the Chinese approach, see T. WANG, *International Law in China: historical and contemporary perspectives*, in *Collected Courses of The Hague Academy of International Law*, vol. 221, 1990, p. 195 ff.; H. XUE, *Chinese Contemporary Perspectives on International Law*, in *Collected Courses of The Hague Academy of International Law*, vol. 355, 2012, p. 41 ff.; P. ROSSI, *China*, in F.M. PALOMBINO (ed.), *Duelling for Supremacy: International Law vs. National Fundamental Principles*, Cambridge, 2019, p. 58 ss.; Z. HE, L. SUN, *A Chinese Theory of International Law*, Singapore, 2020; J. WANG, H. CHENG, *China's Approach to International Law: From Traditional Westphalianism to Aggressive Instrumentalism in the Xi Jinping Era*, in *The Chinese Journal of Comparative Law*, 2022, p. 140 ff.; for an overview of the Soviet and Russian approaches see, S. KRYLOV, Les notions principales du droit des gens (La doctrine soviétique du droit international), in *Collected Courses of The Hague Academy of International Law*, vol. 70, 1947, p. 407 ff.; L. MÄLKSOO, *Russian Approaches to International Law*, Oxford, 2015; Völkerrechtsblog Symposium on "Russian Approaches to International Law", 2018, available at www.völkerrechtsblog.org; M. SMIRNOVA, *Russia*, in F.M. PALOMBINO (ed.), *Duelling for Supremacy: International Law vs. National Fundamental Principles*, Cambridge, 2019, p. 297 ff.; L. MÄLKSOO, R. LESAFFER, *Soviet Approaches to International Law*, in R. KOLB, M. MILANOV (eds.) *The Cambridge History of International Law*, Cambridge, 2025, p. 686 ff.

[15] T. WANG, *International Law in China: historical and contemporary perspectives*, cit., p. 288 ff.; H. XUE, *Chinese Contemporary Perspectives on International Law*, cit., p. 88 ff.; M. A. CARRAI, *Sovereignty in China: A Genealogy of a Concept since 1840*, Cambridge, 2019; J. COHEN, *China's Attitudes Towards International Law – and Our Own*, in J. COHEN (ed.), *Contemporary Chinese Law,* Cambridge, 1970, p. 283 ff.; L. MÄLKSOO, *Russian Approaches to International Law*, cit., p. 100 ff.

[16] Notably, they have been first included in the Preamble of the Agreement between China and the Republic of India on the Trade and Intercourse Between the Tibet Region of China and India of 29 April 1954 and in the final declaration of the 1955 Bandung Conference, considered the manifesto of the Non-Aligned Movement. See T. WANG, *International Law in China: historical and contemporary perspectives*, cit., p. 263 ff.

of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations ("1970 Declaration on Principles of International Law concerning Friendly Relations"): adopted by the UN General Assembly amid Cold War and decolonization dynamics, it further elaborates on the Charter's principles by explicitly prohibiting both direct and indirect intervention in the internal or external affairs of any State[17]. Taken together, these three sources are systematically cited by China and Russia to underpin a vision of international order grounded in the primacy of State sovereignty.

This invocation of sovereignty in Sino-Russian Joint Statements and practice is far from neutral, as it extends well beyond the conventional definition of sovereignty as «supreme authority within a territory»[18]. Instead, it carries with it a set of implications that, as foundational elements of the Sino-Russian conception of international law, constitute the building blocks of a broader critique of the Western-centric international legal order.

This critique has been most clearly articulated in international fora on the application of international law to cyberspace, where China and Russia have actively sought to translate these principles into concrete legal provisions. In this regard, it is no coincidence that they consistently emphasize that core principles such as non-interference, sovereign equality, and the prohibition of the use of force must also govern state behaviour in the information space[19]. On this point, while Western States have also agreed that the principle of sovereignty applies to cyberspace, as testified by the inclusion of this stance in the Tallinn Manual, the divergence with the Sino-Russian approach lies in the implications of that principle, the corollaries it entails, and the rules that should stem from it[20].

In light of the above, this article aims to demonstrate how the Sino-Russian conception of international law, grounded in the principle of sovereignty and its related corollaries, has consistently informed their positions in international cyber fora, first through their proactive efforts to shape the normative framework on cybersecurity, and later through their proposals during the negotiation of the UN Cybercrime Convention, which, to some extent, are also reflected in the treaty's final provisions. To this end, each section of the article will first outline one of these corollaries, then examine how it has been operationalized by China and Russia through regional and universal cooperation on cybersecurity, and finally analyze how

---

[17] UNGA Res 2625(XXV), *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, UN Doc A/RES/2625(XXV).

[18] As in S. BESSON, *Sovereingty*, in *Max Planck Encyclopedia of Public International Law*, 2011.

[19] See, for example, PRESIDENT OF RUSSIA, *Joint Statement of the Russian Federation and the People's Republic of China on the Twentieth Anniversary of the Treaty of Good Neighbourliness and Friendly Cooperation between the Russian Federation and the People's Republic of China*, 28 June 2021, available at www.static.kremlin.ru, ('2021 Joint Statement'), n. III and PRESIDENT OF RUSSIA, *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*, 4 February 2022, available at www.en.kremlin.ru ('2022 Joint Statement'), n. III, see also A. SEGAL, *China's Vision for Cyber-Sovereignty and the Global CyberSovereignty*, in *The National Bureau of Asian Research*, 25 August 2020, available at www.nbr.org. For a comprehensive explanation of how the Five Principles of Peaceful Coexistence should be translated into the rules governing cyberspace according to China's conception of international law, see L. ZHU, W. CHEN, *Chinese Approach to International Law with Regard to Cyberspace Governance and Cyber Operation: From the Perspective of the Five Principles of Peaceful Co-existence*, in *Baltic Yearbook of International Law*, 2023, p. 187 ff.

[20] See M. N. SCHMITT (ed.), *Tallinn Manual 2.0 on the international law applicable to cyberoperations, NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge, 2016, p. 103. More in detail, for the issue of sovereignty in the Western conception of cyberspace, see M. N. SCHMITT, L. VIHUL, *Respect for Sovereignty in Cyberspace*, in *Texas Law Review*, 2017, p. 1639 ff. and A. LIAROPOULOS, *Exercising State Sovereignty in Cyberspace*, in *Journal of Information Warfare: An International Cyber-Order Under Construction?*, 2013, p. 19 ff.

it has been transposed, both in the proposals advanced during the negotiation process and in the final text of the UN Cybercrime Convention.

Notably, the second section will explore the principle of sovereign equality of States, beginning with its interpretation within the Sino-Russian conception of international law and then examining how this understanding has shaped Sino-Russian engagement in UN fora, initially in the field of cybersecurity and subsequently in the negotiations preceding the adoption of the UN Cybercrime Convention. The third section will assess the implications of the Sino-Russian notion of sovereignty for the international protection of human rights, demonstrating how it has resulted, both in cybersecurity cooperation and in the context of the UN Cybercrime Convention, in the subordination of online rights and freedoms to State interests. The fourth section will turn to the principle of non-interference in internal affairs, as derived from the Sino-Russian understanding of sovereignty, highlighting how this principle has been advanced through joint cybersecurity initiatives and further embedded in the normative proposals put forward in the UN Cybercrime Convention. Finally, the fifth section will conclude.

2. *The Cybercrime Convention as the result of Sino-Russian activism in UN cyber fora: mirroring equal participation in international lawmaking as a corollary of sovereign equality*

2.1. *Sovereign equality and equal participation in international lawmaking in the Sino-Russian approach to international law*

According to the classical teaching of international law, if one State is able to impose its will upon another and thereby place itself in a position of superiority, the very notion of sovereignty is undermined; thus, equality must be regarded as an intrinsic condition of sovereignty[21]. While this principle should constitute one of the foundational elements of the international legal order, as enshrined in the United Nations Charter, the post-war institutional framework reflects the substantial disparities in economic and political power among States, which are mirrored in the rules of international law[22].

It is precisely in response to this reality that Sino-Russian practice places strong emphasis on the substantive equality of States, framing it as a principle through which to challenge the international legal order marked by deep structural inequality[23]. In this vein, equality figures prominently in the three normative sources most frequently invoked in Joint Sino-Russian Statements on international law: among the Five Principles of Peaceful Coexistence is the principle of «equality and mutual benefit»[24]; the United Nations Charter opens the list of founding principles in Article 2 with a reaffirmation of the sovereign equality of all its member States and the 1970 Declaration on Principles of International Law

[21] R. P. ANAND, *Sovereign Equality of States in International Law*, in *The Hague Academy of International Law Collected Courses*, vol. 197, 1986, p. 22.
[22] A. ANGHIE, *Imperialism, Sovereignty, and the Making of International Law*, Cambridge, 2005; G. SIMPSON, *Great Powers and Outlaw States: Unequal Sovereigns in the International Legal Order*, Cambridge, 2004.
[23] T. CHEN, *The People's Republic of China and Public International Law*, in *Dalhousie Law Journal*, 1984, pp. 25-26; L. MÄLKSOO, *Russian Approaches to International Law*, cit., p. 100 ff.
[24] L. FOCSANEANU, *Les cinq principes de coexistence et le droit international*, in *Annuaire français de droit international*, 1956, pp. 174-177.

concerning Friendly Relations solemnly declares that «every State has the duty to promote, through joint and separate action, realization of the principle of equal rights»[25].

In the Sino-Russian Joint Statements of 2016[26]and 2025[27], sovereign equality is understood to require the active participation of all States in the development of international law, explicitly opposing a norm-setting process driven solely by Western powers[28]. Thus, while the existing body of international law is the product of a Western-centric order, in fields where international legal norms are still evolving China and Russia assert their right to play a direct and influential role in shaping the legal framework, having «the right to participate in the making of, interpreting and applying international law on an equal footing [...]»[29].

This position is justified through the recourse to two core, though at times conflicting, concepts emerging from Sino-Russian practice.

The first is the idea of democracy, not understood as internal political democracy, but as a form of international democratic order; namely, democracy among States[30]. According to this stance, international law can only be truly "international" if it results from negotiations in which all States are equally represented and able to influence outcomes[31]. Only through such inclusive participation can the resulting standards be considered genuinely global, rather than reflecting the preferences of a select group of hegemons[32]. This logic underpins the Chinese and Russian insistence that the United Nations, where all States have a voice, is the only legitimate forum for multilateral lawmaking.

The second concept is that international legal norms must reflect a balance between the major poles of global power; essentially, a concert of great powers, particularly the permanent members of the UN Security Council[33]. While this notion of great power coordination may seem at odds with the principle of sovereign equality, in practice both ideas serve to justify a more assertive role for Russia and China in international norm-making. Whether grounded in a call for equal participation or in the recognition of the necessity of balance of powers, both doctrines converge in supporting their claim to a seat at the lawmaking table[34].

---

[25] UNGA Res 2625(XXV), *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations* , cit. pp. 133-134.

[26] MINISTRY OF FOREIGN AFFAIRS OF RUSSIAN FEDERATION, *The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law*, 25 June 2016, available at www.mid.ru ('2016 Joint Declaration'), para. 2.

[27] EMBASSY OF THE PEOPLE'S REPUBLIC OF CHINA IN THE UNITED STATES OF AMERICA, *Joint Declaration of the People's Republic of China and the Russian Federation on Further Strengthening Cooperation to Uphold the Authority of International Law*, 9 May 2025, available at www.us.china-embassy.gov.cn ('2025 Joint Declaration'), n. 5.

[28] I. WUERTH, *China, Russia, and International Law*, in *Lawfare*, 11 July 2016, available at www.lawfareblog.com.

[29] 2016 Joint Declaration, para. 2; 2025 Joint Declaration, para. 5.

[30] J. KU, *What Does China Mean When It Celebrates the "International Rule of Law"?*, in *Opinio Juris*, 29 October 2014, available at www.opiniojuris.org; 2022 Joint Statement, n. I.

[31] See former Chinese Foreign Minister speech, Y. WANG, *China: A Staunch Defender and Builder of International Rule of Law*, in *Chinese Journal of International Law*, 2014, p. 638.

[32] PRESIDENT OF THE PEOPLE'S REPUBLIC OF CHINA, *Carry forward the Five Principles of Peaceful Coexistence to build a better world through win-win cooperation*, 28 June 2014, available at www.china.org.cn.

[33] A. ROBERTS and M. KOSKENNIEMI, *Is International Law International?*, Oxford, 2017, p. 294 and MINISTRY OF FOREIGN AFFAIRS OF RUSSIAN FEDERATION, *Concept of the Foreign Policy of the Russian Federation*, 18 February 2013, available at www.mid.ru., para. 4.

[34] L. MÄLKSOO, *Russia and China Challenge the Western Hegemony in the Interpretation of International Law*, in *Ejil:Talk!*, 15 July 2016, available at www.ejiltalk.org.

2.2. *Sino-Russian activism in UN cybersecurity and cybercrime fora: contesting the application of "Western-centred" norms through equal participation in shaping emerging international law*

It is no coincidence, then, that this demand for participation has found one of its clearest expressions in the debate over the application of international law to cyberspace. Cyberspace is seen by both Russia and China as a domain where legal standards remain unsettled and still open to negotiation and influence. Therefore, within relevant UN fora, Russia, China, and States with a similar perspective have consistently opposed the automatic application of existing international legal norms to cyberspace, advocating instead for the negotiation of new rules that better reflect a multipolar world order[35].

The need to address the application of international law to cyberspace, indeed, was placed on the UN agenda in 1998, following a Russian initiative[36]. These efforts led to the establishment of the *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UN GGE)[37] in 2006, and later, the *Open-Ended Working Group* (OEWG)[38] on the same topic in 2018. In these fora, Russia and China have consistently sought to prevent the automatic application of existing international legal rules to cyberspace, leading to ongoing tensions and opposition from the so-called "Western bloc"[39]. This persistent obstructionism has resulted in a deepening divide between positions[40] and universal consensus has been reached solely on the general principle that international law applies to cyberspace[41].

---

[35] A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023, p. 11 ff.

[36] PERMANENT REPRESENTATIVE OF RUSSIAN FEDERATION TO THE UN, Letter dated September 23, 1998 addressed to the Secretary-General, U.N. Doc. A/C.1/53/3. The proactive role of Russia was indeed instrumental in the adoption of UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/53/70 of 4 January 1999. Russia's role was also pivotal in the following years, with a number of proposals on the matter then adopted by the UNGA. See UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/54/49 of 23 December 1999, UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/55/28 of 20 December 2000 e UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/56/19 of 7 January 2002.

[37] UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/60/45 of 6 January 2006, para. 4.

[38] UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/73/27 of 11 December 2018.

[39] This approach is summarized by *Statement by the Representative of the Russian Federation at the fourth session of the UN Open-ended Working Group on Security of and in the use of ICTS 2021-2025*, 7 March 2023, available at www.unoda.org. A symbolic moment in this clash occurred in 2017 during the OEWG discussions on countermeasures, self-defence, and the applicability of international humanitarian law in cyberspace. Due to the stark divisions among participating States, the group failed to adopt a final report, on which see M. SCHMITT and L. VIHUL, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, in *Just Security*, 2017, available at www.justsecurity.org.

[40] With few exceptions, such as the progresses reached during the 2021 session, on which see M. SCHMITT, *The Sixth United Nations GGE and International Law in Cyberspace*, in *Just Security*, 2021, available at www.justsecurity.org.

[41] On the applicability of international law to cyberspace, see UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98 of 24 June 2013, para. 8; UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc

Complementing this resistance to the application of existing rules is the parallel effort by Russia and China to promote the adoption of new, specific rules for cyberspace. National positions have been first coordinated within the Shanghai Cooperation Organization (SCO)[42], a regional organization focused primarily on security and comprising China, Russia, the Central Asian States, India, Pakistan, and Iran, and then proposed at the United Nations[43].

In line with this strategy, the SCO launched its *Plan of Action to Ensure International Information Security*[44], which laid the foundation for the 2009 Agreement on Cooperation in the Field of Information Security[45]. Building on these regional initiatives, SCO member States, led by Russia and China, submitted non-binding Codes of Conduct to the United Nations in 2011[46] and, with some revisions[47], again in 2015[48]. These proposals were built around some clear core elements: the emphasis on the driving role of the United Nations, as the appropriate forum for cybersecurity negotiations[49]; a focus on State sovereignty, equitable distribution of cyber resources between States, and non-interference in the internal affairs[50]; the need to cooperate and exchange information to combat cybercrime, including the "dissemination of information that incites terrorism, separatism and extremism"[51]; a preference for a multilateral rather than a multistakeholder approach, with a driving role of

A/70/174 of 22 July 2015, para. 12; UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc A/76/135 of 14 July 2021, para. 17. For the OEWG, see UN General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report*, UN Doc A/AC.290/2021/CRP.2 of 10 March 2021, para. 2. On this approach by China and Russia, see A. HENRIKSEN, *The End of the Road for the UN GGE Process and the Future Regulation of Cyberspace*, in *Journal of Cybersecurity*, 2019, p. 3.

[42] For a detailed description of this pattern, see A. MARICONDA, P. ROSSI, *The Shanghai Cooperation Organization and Cybersecurity: A Sino-Russian Approach to International Law?*, in *I Quaderni della Comunità Internazionale, Quaderno 29 - Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, 2024, p. 265 ff.; more in detail on Sino-Russian regional efforts, see L. KHASANOVA, A. SIMONYAN, *(Geo)politicizing International Law of Cyberspace in Post-Soviet Eurasia*, in *Chinese Journal of International Law*, 2025.

[43] See B. TOSO DE ALCANTARA, *SCO and Cybersecurity: Eastern Security Visions for Cyberspace*, in *International Relations and Diplomacy*, 2018, p. 549 ff.; E. MIKHAYLENKO, A. OSPANOVA, M. LAGUTINA, *The SCO and Security Cooperation*, in S. MAROCHKIN, Y. BEZBORODOV (eds.), *The Shanghai Cooperation Organization: Exploring New Horizons*, London, 2022, p. 44 and Y. HU, *The Role of the SCO in the Progressive Development of International Legal Norms in the Field of Information Security,* in *Frontiers in Business, Economics and Management*, 2024, p. 356 ff.

[44] U.N. General Assembly, *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General*, U.N. Doc. A/64/129, 8 July 2009, reply received from Kazakhstan, para. 9.

[45] *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, signed on 16 June 2009* at Ekaterinburg ("SCO 2009 Information Security Agreement". The text is available at www.sectsco.org.

[46] UN General Assembly, *Letter dated 2011/09/12 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, UN Doc. A/66/359 of 12 September 2011.

[47] The Citizen Lab at the University of Toronto developed an interactive tool for comparing the two Draft Codes, available at www.openeffect.ca.

[48] UN General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, UN Doc. A/69/723 of 13 January 2015.

[49] *Letter dated 2011/09/12*, cit., lett. j); *Letter dated 9 January 2015*, cit., n. 12

[50] *Letter dated 2011/09/12*, cit., letts. a), b) and g); *Letter dated 9 January 2015*, cit., nos. 1, 3 and 8.

[51] *Letter dated 2011/09/12,* cit., lett. c.); *Letter dated 9 January 2015*, cit., no. 4

the State[52]; and a tendency to subordinate human rights in the digital domain to national security and strategic interests[53].

It is precisely these features that provoked strong opposition from the "Western bloc" and ultimately led to the General Assembly's decision not to adopt either of the proposed codes[54]. As previously mentioned, indeed, States opposing the SCO's approach to cybersecurity favour the application of existing international legal norms to cyberspace, rather than the creation of new, customized rules or codes of conduct[55]. They also express concern over the subordination of human rights to national legislation[56] and emphasize the importance of involving private stakeholders in cyber governance, given the significant role played by private companies in this domain[57].

Following the failure of these initiatives, aside from a few bilateral efforts that continued to focus on information security[58], China and Russia sought to revive the same set of priorities by "shoehorning"[59] them under the different label of international cooperation on cybercrime[60]. In fact, their joint efforts in this field intensified in the years immediately after the UN General Assembly declined to adopt the proposed cybersecurity codes of conduct. Russia, in particular, invested significant diplomatic energy in establishing the AHC, which was ultimately created by the General Assembly in 2019, and in pushing for the negotiation of a binding treaty within that framework[61].

---

[52] *Letter dated 2011/09/12*, cit., letts. g) and h); *Letter dated 9 January 2015*, cit., nos. 8 and 9.

[53] *Letter dated 2011/09/12*, cit., lett. f); *Letter dated 9 January 2015*, cit., no. 7

[54] For a complete overview of the disagreement between the "Western Bloc" and Sino-Russian view of international legal framing of cybersecurity, see A. ROBERTS, M. KOSKENNIEMI, *Is International Law International?*, cit., p. 306 ff.

[55] See, for example, US *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World*, May 2011, p. 9 and United Kingdom, *Response to General Assembly resolution 68/243 Developments in the field of information and telecommunications in the context of international security*, 2014, available at www.ccdcoe.org. As for scholarship, see T. MAURER, *Cybernorms Emergence at the United Nations – An Analysis of the Activities at the UN regarding Cybersecurity*, in *Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project of Harvard Kennedy School*, 2011, pp. 25-26; J. A. LEWIS, *Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms, Report of the Center for Strategic and International Studies*, 2014, available at www.csis.org; M. KALJURAND, *United Nations Group of Governmental Experts: The Estonian Perspective*, in A. M. OSULA, H. ROIGAS (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, 2016, p. 123 and, as for scholarly skepticism, see J. Goldsmith, *Cybersecurity Treaties: A Skeptical View*, in *Lawfare*, 9 March 2011, available at www.lawfaremedia.org.

[56] See PETERS, H. KRIEGER and L. KREUZER, *Due Diligence: The Risky Risk Management Tool in International Law*, in *Cambridge International Law Journal*, 2020, 134-135 and J. KENNY, *Cyberoperations and the Status of due diligence obligations in International Law*, in *International and Comparative Law Quarterly*, 2023, pp. 169-170.

[57] See, on this approach to cybersecurity governance; K. E. EICHENSEHR, *The Cyber-Law of Nations*, in *Georgetown Law Journal*, 2015, p. 330 ff.; C. KAUFFMANN, *Multistakeholder Participation in Cyberspace*, in *Schweizerische Zeitschrift für internationales und europäisches Recht,* 2016, p. 217 ff.

[58] Notably, China and Russia signed a bilateral treaty in 2015, which reflects the same priorities of the 2009 SCO Agreement, signed on 30th April 2015, whose English translation is available at www.cyber-peace.org; for a commentary of this treaty, see A. SEGAL, *Peering into the future of Sino-Russian cybersecurity cooperation*, in *Texas National Security Law Review*, 10 August 2020, available at www.warontherocks.com; moreover, China signed a bilateral treaty with the USA in 2015, signed on 25th September 2015, whose text is available at www.obamawhitehouse.com.

[59] See A. SUKUMAR and A. BASU, *Back to the territorial state*, cit., p. 264.

[60] On the fragmentation of the international legal regimes in the cyber domain, see J. NYE, *The Regime Complex for Managing Global Cyber-activities*, in *Global Commission on Internet Governance Paper Series 1*, 2014.

[61] See K. GULLO and K. RODRIGUEZ, *UN Cybercrime Draft Treaty Timeline*, in *Electronic Frontier Foundation*, 2023, available at www.eff.org.

Once again, this process has mirrored the broader divide between the "Western bloc" and the Sino-Russian approach to cyberspace governance. The main existing international instrument in the fight against cybercrime, the "Budapest Convention"[62], was developed under the auspices of the Council of Europe and has never been ratified by either Russia or China. Both countries have long criticized its content and have instead advocated the creation of a parallel treaty negotiated within the United Nations, which they regard as the only appropriate forum for such efforts[63]; Russian and Chinese activism has materialized in six treaty proposals, submitted either jointly or separately, which culminated in the adoption of a draft treaty by the UN General Assembly on 24 December 2024.

The substance of this draft and the ways in which it reflects the Sino-Russian vision of international law will be explored in the following sections. What is important to emphasize here is that the very adoption of the UN Cybercrime Convention, after two decades of sustained Sino-Russian diplomatic activism at the United Nations[64], can be considered a direct reflection of their shared vision of international law. Despite being presented under the different labels of "cybersecurity" and "cybercrime", China and Russia have consistently advocated for the development of specific legal frameworks for cyberspace, rejecting the simple extension of existing international law to it[65]. This is perhaps the clearest expression of the idea articulated in the Sino-Russian declarations on international law: that sovereign equality, as a fundamental principle of international law, entails the equal participation of all States in the drafting of international legal norms.

3. *The over-broad powers of the State in repressing cybercrime: mirroring the subordination of human rights to State sovereignty*

3.1. *The interplay between State sovereignty and human rights in the Sino-Russian approach to international law*

The centrality of sovereignty in the Sino-Russian conception of international law also shapes the distinctive approach both countries take to the protection of human rights. In its internal dimension, indeed, sovereignty essentially translates into «the supreme power of the State over its territory and the persons and things within its territorial limits»[66]. As made explicit in China's First National Cybersecurity Strategy of 2016, the States in question

---

62 Council of Europe, Convention on Cybercrime (ETS No. 185), opened for signature on 23/11/2001, Budapest.

63 For the Russian position, see MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION, *International Community has Come Closer to 'Cybercrime' Vaccine*, in *Ministry of Foreign Affairs of the Russian Federation*, available at www.mid.ru; for the Chinese position, see E.S. ZHANG and R. CREEMERS, *Towards a UN-Centric Cybercrime Treaty: Chinese positions and interests at the UN Ad Hoc Committee for a cybercrime convention,* 2024, available at www.leidenasiacentre.nl.

64 On which see A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, cit., p. 11 ff. and H. TIRMA-KLAAR, *The Evolution of the UN Group of Governmental Experts on Cyber Issues*, in *Cyberstability Paper Series – New Conditions and Constellations in Cyber*, The Hague Center for Strategic Studies, available at www.hcss.nl.

65 For the different perspectives on internet governance in international law, see G. M. RUOTOLO, *Abolish the Rules Made of Stone? Contemporary International Law and the models to Internet Regulations*, in *Italian Review of International and Comparative Law*, 2022, p. 254 ss.

66 T. WANG, *International Law in China: historical and contemporary perspectives*, cit., p. 297.

consider cyberspace to be «the nation's new territory for sovereignty»[67]. It is therefore particularly significant to examine how this conception of State authority, extended to include cyberspace, interacts with the very limitation traditionally imposed on such authority: the obligation to respect human rights.

In Russian legal scholarship, following the collapse of the Soviet Union, a theoretical debate emerged between the classical/statist school of international law and a more individual-centered perspective[68]. Over time, the statist view has come to shape the dominant legal and institutional narrative: as reflected, for instance, in public statements by the President of the Constitutional Court, sovereignty is understood as absolute and indivisible and may be limited only through the express consent of the State[69]. Thus, according to the prevailing view, the Westphalian model must continue to serve as a guiding framework, and the protection of human rights (along with the principle of self-determination) must not be allowed to become a tool through which Western schools of thought erode the full sovereignty of the State[70].

The clearest practical expression of this approach can be found in Russia's relationship with the European Court of Human Rights (ECtHR). Following the incorporation of human rights into the Russian Constitution in the '90s, Russia acceded to the European Convention on Human Rights (ECHR) and Western Europe viewed this development as a chance to improve the country's human rights record[71]. However, tensions soon emerged, particularly after a series of ECtHR judgments concerning the protection of rights considered incompatible with Russian national identity[72]. In response, the Russian Constitutional Court was vested with the authority to assess the compatibility of ECtHR rulings with Russia's

---

67 CYBERSPACE ADMINISTRATION OF CHINA, *National Cyberspace Security Strategy*, 27 december 2016, English translation available at www.dig.watch.

68 L. MÄLKSOO, *Russian Approaches to International Law*, cit., pp. 101-103, who, in summarizing this debate within Russian-language international law scholarship, notes that the statist school of international law remains dominant in major academic centers closely aligned with State power, whereas the more "individualist" school, shaped by Western legal thought, is largely confined to more peripheral contexts.

69 Ibid., p. 102, in which the author cites as an example the programmatic article on international law of the President of Russian Costitutional Court Zorkin, titled "An Apology for the Westphalian Sytem".

70 This refers in particular to those schools of thought, primarily in the United States, that link sovereignty and the protection of human rights, asserting that true sovereignty cannot exist without respect for the latter. See, for example, M. W. REISMAN, *Sovereignty and Human Rights in Contemporary International Law*, in *American Journal of International Law*, 1990, p. 866 ff.

71 On the limited impact of the case law of the ECtHR on Russian legal system, see L. MÄLKSOO, W. BENEDEK (eds.), *Russia and the European Court of Human Rights. The Strasbourg Effect*, Cambridge, 2017.

72 Scholars often highlight three landmark cases in the dialectic between the ECtHR and the Russian Constitutional Court: *Kostantin Markin v. Russia*, 22 March 2012, Application no. 30078/06, where the Court condemned Russia for denying equal family benefits to a male military officer, seen as contrary to traditional Russian family values; *Anchugov and Gladkov v. Russia*, 9 December 2013, Applications nos. 11157/04 and 15162/05, which addressed the voting rights of prisoners and the landmark *Oao Neftyanaya Kompaniya Yukos v. Russia*, 31 July 2012, Application no. 14902/04, concerning the alleged politically motivated expropriation of an oil company; See M. BALBONI, C. DANISI, *Reframing Human Rights in China and Russia: How National Identity and National Interests Shape Relations with, and the Implementation of, International Law*, in S. BIANCHINI, A. FIORI (eds.), *Rekindling the strong State in Russia and China*, Leiden, 2020, p. 61 ff.; S. MAROCHKIN, *ECtHR and the Russian Constitutional Court: duet or duel?*, in L. MÄLKSOO, W. BENEDEK (eds.), *Russia and the European Court of Human Rights*, cit., p. 93 ff.; A. TROCHEV, *The Russian Constitutional Court and the Strasbourg Court: judicial pragmatism in a dual State*, in L. MÄLKSOO, W. BENEDEK (eds.), *Russia and the European Court of Human Rights*, cit., p. 125 ff.

constitutional values[73]. Exercising this power, the Court held that any judgment from Strasbourg found to be in conflict with these values should not be enforced, as doing so would violate the principle of sovereignty, which it considers as a *jus cogens* norm[74]. As is well known, this already fraught relationship deteriorated further with Russian invasion of Ukraine, leading to Russia's expulsion from the Council of Europe and, consequently, from the Convention itself[75].

In short, although Russia has pursued a degree of integration into the international human rights framework, it has consistently subordinated it to what it considers the supreme value of international law: State sovereignty; and this has resulted in a fundamentally nationalist and anti-universalist interpretation of human rights[76].

As for China, its approach to human rights is deeply shaped by its historical trajectory. During the Maoist era, the dominant collectivist ideology left little room for the concept itself of human rights, which were widely regarded as a Western deviation[77]. Since the opening-up reforms of the late 1970s, China has adopted a dual approach: on the one hand, it has joined far fewer international human rights treaties than Russia; on the other, it has developed its own discourse and theoretical framework on human rights, rooted in its unique historical and cultural experience[78]. According to this perspective, human rights are not seen as individual legal entitlements but rather as both a "cause and a process": they are understood as objectives to be achieved progressively through social development, rather than pre-existing rights that can be applied universally and abstractly; individual rights, in this view, cannot be meaningfully realized without specific social conditions, and must always be understood within their broader societal context[79].

This framework leads to two defining features of China's human rights narrative: first, a rejection of the notion that human rights are universally applicable in a context-independent way, emphasizing instead the importance of cultural and social specificity; second, the primacy of collective welfare over individual freedoms[80]. This emphasis implies that individual rights may be legitimately restricted when doing so serves the greater good,

---

[73] Law of the Russian Federation amending the Law on the Constitutional Court no. 1-FKZ of 21 July 1994, entered into force on 15 December 2015.

[74] Judgment of 14 July 2015, No 21-П/2015, on which see L. MÄLKSOO, *Russia's Constitutional Court Defies the European Court of Human Rights: Constitutional Court of the Russian Federation Judgment of 14 July 2015, No 21-П/2015*, in *European Constitutional Law Review*, 2016, p. 377 ff.; M SMIMOVA, *Russian Constitutional Court Affirms Russian Constitution's Supremacy over ECtHR Decisions*', in *EJIL: Talk!*, 15 July 2015, available at www.ejiltalk.org; M AKSENOVA, *Anchugov and Gladkov is not Enforceable: the Russian Constitutional Court Opines in its First ECtHR Implementation Case*, in *Opinio Juris*, 25 April 2016, available at www.opiniojuris.org; A. CALIGIURI, *La recente giurisprudenza costituzionale russa sui rapporti tra Convenzione europea dei diritti umani e ordinamento interno*, in *Diritti umani e diritto internazionale*, 2016, p. 703 ff.

[75] See A. SACCUCCI, *Le conseguenze dell'espulsione della Russia dal Consiglio d'Europa sui trattati stipulati nell'ambito dell'organizzazione*, in *Diritti Umani e Diritto Internazionale*, 2022, p. 211 ff.

[76] L. MÄLKSOO, *Russia and European Human-Rights Law: Margins of the Margin of Appreciation*, in *Review of Central and East European Law*, 2012, p. 359 ff.

[77] H. CHIU, *Chinese Attitudes toward International Law of Human Rights in the Post-Mao era*, in V.C. FALKENHEIM (ed.) *Chinese Politics from Mao to Deng*, New York, 1989, p. 237 ff. and B. AHL, *The Rise of China and International Human Rights Law*, in *Human Rights Quarterly*, 2015, p. 637 ff.

[78] S. SCEATS, S. BRESLIN, *China and the International Human Rights System*, Londra, 2012.

[79] H. XUE, *Chinese Contemporary Perspectives on International Law*, cit., p. 125 ff.

[80] S.P. SUBEDI, *China's Approach to Human Rights and the UN Human Rights Agenda*, in *Chinese Journal of International Law*, 2015, p. 437 ff.

placing particular weight on economic and social rights rather than civil and political liberties[81].

Thus, although grounded in distinct historical experiences and shaped by differing doctrinal approaches, both Russian and Chinese approaches to human rights ultimately converge on a common legal position: since human rights are not generally recognized as foundational principles of international law, when a conflict arises between the protection of human rights and one of these core principles, sovereignty above all, it is the latter that is understood to prevail[82].

This convergence is clearly reflected in the Joint Statements and the three main sources cited therein: in all of them, sovereignty occupies a central position, while human rights are conspicuously absent. The Five Principles make no mention of them at all; in the UN Charter, they appear only among its general purposes in Article 1, not among the principles listed in Article 2, which are the ones consistently cited in Sino-Russian declarations[83]; and in the 1970 Declaration on Principles of International Law concerning Friendly Relations, human rights are not included among the operative principles themselves, but are merely referenced in the preamble. This selective invocation of sources goes hand in hand with a similarly selective approach to the way human rights themselves are addressed in Joint Statements: at times, they are omitted altogether[84]; in others, they are referenced only to stress the need to counter the politicization of the international human rights agenda, to abandon double standards, and to interpret rights within specific cultural and historical contexts[85], while warning against their use «to put pressure on other countries»[86]. Taken together, these elements reveal a coherent pattern in which the centrality of sovereignty serves as a subtle yet deliberate contestation of the international human rights regime, thereby promoting the prioritization of national interests over the protection of individual rights, using the concept of sovereignty as the vehicle through which this legal stance is articulated[87].

This entails that when vaguely defined vital interests of the State are threatened by individual actions, such actions must be suppressed, even at the cost of violating human rights as they are generally understood. A clear example of this concept is the campaign that Russia and China are carrying out against what they call the "three evils": terrorism, separatism, and extremism[88]. Without ever precisely defining what these terms encompass, both countries, and the SCO as a key platform of cooperation between them[89], reference

---

[81] M. BALBONI, C. DANISI, *Reframing Human Rights in China and Russia: How National Identity and National Interests Shape Relations with, and the Implementation of, International Law*, cit., p. 74.

[82] Ibid. and M. XINMIN, *International Law Issues in Cyberspace*, in *Chinese Yearbook of International Law*, 2015, pp. 542-545.

[83] L. MÄLKSOO, *Russia and China Challenge the Western Hegemony in the Interpretation of International Law*, cit.

[84] 2016 Joint Declaration and 2025 Joint Declaration.

[85] 2022 Joint Statement, n. I.

[86] 2021 Joint Statement, n. I; 2022 Joint Statement, n. I

[87] B. AHL, *The Rise of China and International Human Rights Law*, cit., p. 637 ff.; B. HARZL, *Nativist ideological responses to European/liberal human rights discourses in contemporary Russia*, in L. MÄLKSOO, W. BENEDEK (eds.), *Russia and the European Court of Human Rights: The Strasbourg Effect*, cit., p. 355 ff.

[88] E. LI, *Fighting the "Three Evils": A Structural Analysis of Counter-terrorism Legal Architecture in China*, in *Emory International Law Review*, 2019, p. 365 ff.

[89] S. ARIS, *The Shanghai Cooperation Organisation: "Tackling the Three Evils". A Regional Response to Non-Traditional Security Challenges or an Anti-Western Bloc?*, in *Europe-Asia Studies*, 2009, p. 457 ss.

them extensively in their acts, using them as powerful tools to make vague accusations against dissidents and minorities, accused of undermining the sovereign interests of the State[90].

Lastly, given the importance of the interests at stake, such conducts are viewed as inherently affecting State sovereignty and, therefore, must be prosecuted also extraterritorially. Based on this principle, Russia has engaged in well-known acts of extraterritorial repression, including the assassination of dissidents abroad[91]. Similarly, China has attempted to assert extraterritorial jurisdiction, particularly under the "effects doctrine"[92], that is, the claim of jurisdiction over conduct occurring abroad on the grounds that it allegedly produces harmful effects within the State's own territory, targeting dissidents and members of minorities living overseas[93].

In short, under the Sino-Russian conception of sovereignty, State interests take precedence over human rights. This justifies the suppression, even beyond national borders, of conduct vaguely defined as "terrorism, separatism, and extremism", solely on the basis of its perceived impact on the sovereignty of the State.

3.2 *The subordination of human rights to State imperatives in the Sino-Russian practice on "information security"*

One of the domains in which both Russia and China first sought to give concrete form to this conception of the relationship between sovereignty and the protection of human rights is cybersecurity. In this regard, they prefer the term *information security* over *cybersecurity*: this choice reflects the view that cyberspace should be subject to State control over the flow of information[94]. In essence, in contrast to the Western conception of cybersecurity, which focuses primarily on the technical protection of systems, software, and data from accidental or malicious threats, the concept of information security also includes the regulation of online content considered harmful to political, economic, or social stability[95].

---

[90] In the case of Russia, terrorism, separatism and extremism have been frequently invoked in repressive legislation aimed at silencing activists and NGOs critical of the war against Ukraine, as well as various minority groups within the Russian Federation. In China, the most intensive application of anti-terrorism and anti-extremism laws has taken place in the Xinjiang Uyghur Autonomous Region. There, under vague accusations of separatism and terrorism, often linked to the Islamic faith of the local population, the government has conducted a harsh and systematic campaign of repression against the Uyghur minority. For a detailed description of this legislation, see B. MERETTI, *The 'War On Minorities' Under the Guise of Countering Terrorism and Violent Extremism*, in *Research Brief of the Geneva Academy of International Humanitarian Law and Human Rights*, November 2024, available at www.geneva-academy.ch.

[91] See COUNCIL OF EUROPE, Report by Rapporteur C. Chope, Committee on Legal Affairs and Human Rights, *Transnational repression as a growing threat to the rule of law and human rights*, Doc. 15787, 5 June 2023, p. 11 ff.

[92] Y. XIAO, L. ZHU, *The Effect Doctrine and the Extraterritorial Application of Chinese Law: It's Easier Said Than Done*, in I. DE LA RASILLA, C. CAI (eds.) *The Cambridge Handbook of China and International Law*, Cambridge, 2024, p. 181 ff.

[93] S. GUO, D. IRELAND PIPER, *China and Extraterritorial Criminal Jurisdiction*, in D. IRELAND-PIPER (ed.) *Extraterritoriality in East Asia: Extraterritorial Criminal Jurisdiction in China, Japan, and South Korea*, Cheltenham, 2021, p. 48 ff.

[94] See K. GILES, *Russia's Public Stance on Cyberspace Issues*, in *4th International Conference on Cyber Conflict*, 2012, available at www.ccdcoe.org; C. CUIHONG, *Cybersecurity in the Chinese context: Changing concepts, vital interests, and prospects for cooperation*, in *China Quarterly of International Strategic Studies*, 2015, p. 475 ff.

[95] See, for example, the Annex 1 ("List of Basic Terms in the Field of International Information Security") of the 2009 SCO Agreement on Cooperation in the Field of Information Security, which broadly defines information security as "the status of individuals, society and the state and their interests when they are protected from threats, destructive and other negative impacts in the information space".

Quite revealingly, in Annex 2 ("List of Basic Types, Sources, and Features of Threats in the Field of International Information Security") of the aforementioned 2009 SCO Agreement on Cooperation in the Field of Information Security, «the dissemination of information harmful to the socio-political and socio economic systems, spiritual, moral and cultural environment of other States», vaguely defined as «distorting the picture of the political and social system of a State, its foreign and domestic policy, important political and social processes in the country, spiritual, moral and cultural values of its population»[96] is identified as a major threat to information security. The aim of such vague terminology is precisely to grant governments broad discretion in restricting online content, something that becomes particularly evident when examining the domestic governance of information security in China and Russia[97].

Notably, at the domestic level, both States have developed extensive internal censorship systems that filter online content (the Chinese "Great Firewall of China" and the Russian *Roskomnazor*)[98], subordinating digital freedoms and rights to vague State security imperatives such as the fight against "terrorism, extremism, and separatism"[99].

Such State interference is accompanied by minimal safeguards or guarantees with regard to human rights and freedoms online, consistently subordinating their protection to domestic law, in line with the approach described above. In this context, the clearest examples are the two Codes of Conduct on information security proposed by SCO member States to the United Nations.

The 2011 Code affirms a commitment «to fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate

---

[96] The English translation of this text is available at www.sectsco.org.

[97] For UN Human Rights Treaty bodies criticism towards Russian and Chinese legal framework in this field, see Comments Provided by David Kaye, the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression about People's Republic of China Cybersecurity Law (Draft) Pending Before the 12th National People's Congress, 4 August 2015, available at www.spcommreports.ohchr.com and HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the situation of human rights in the Russian Federation*, UN Doc. A/HRC/54/54 of 15 September 2023, 11, paras. 60-62.

[98] For China, the huge censorship apparatus known as the "Great Firewall of China" answers directly to an organ of the Chinese Communist Party (the Central Leading Group on Network Security and Informatization), and finds its legal basis in the Information Security Law of 2017, which allows limitations on online content based on very vague grounds (the English translation of the law is available at www.digichina.stanford.edu) see, on this issue, G. AUSTIN, *Cybersecurity in China: The next wave*, Cham, 2018 M. SVENSSON, *Human Rights and the Internet in China: new frontiers and challenges*, in S. BIDDULPH, J. ROSENZWEIG (eds.), *Handbook on Human Rights in China*, Cheltenham, 2019, p. 632 ff; M. JIANG, *Cybersecurity Policies in China*, in L. BELLI (ed.), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*, Cham, 2021, p. 183 ff.; R. CREEMERS, *The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy*, in *Journal of Contemporary China*, 2024, p. 173 ff.; Quite similar is the Russian online control system: the *Roskomnazor*, a body subordinate to the executive power that exercises extensive censorship powers based on a number of laws permitting the restriction and blocking of online content based on very vague grounds (see Federal Law of 28.12.2013 N 398-FZ On Amendments to the Federal Law "On Information, Information Technologies and the Protection of Information" and Federal Law of 06.07.2016 N 374-FZ on Amendments to the Federal Law "On Countering Terrorism" and certain legislative acts of the Russian Federation regarding the establishment of additional counter-terrorism measures and ensuring public safety") on which see O. CHISLOVA, M. SOKOLOVA, *Cybersecurity in Russia*, in *International Cyber Security Law Review*, 2021, p. 245 ff.; A. SHCHERBOVIC, *Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the "Sovereignization" of the Internet in Russia*, in L. BELLI (ed.), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*, Cham, 2021, p. 67 ff.

[99] see S. ARIS, *The Shanghai Cooperation Organisation: "Tackling the Three Evils". A Regional Response to Non-Traditional Security Challenges or an Anti-Western Bloc?*, cit.

information," but "*on the premise of complying with relevant national laws and regulations*»[100]. In doing so, it clearly places human rights under the authority of domestic legal frameworks[101]. The 2015 Code, in an attempt to address the criticisms raised by the previous version, adopts a more nuanced language, stating the commitment to «fully respect rights and freedoms in the information space, including the right and freedom to seek, receive and impart information», while emphasizing that the International Covenant on Civil and Political Rights (ICCPR, Article 19) attaches «special duties and responsibilities» to this right and noting that the right «may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (ordre public), or of public health and morals»[102].

Scholars have noted that even this revised formulation remains problematic. First, it selectively cites only the limitations to freedom of expression contained in Article 19(3) of the ICCPR, implicitly suggesting that the State control mechanisms discussed earlier fall within the permissible scope of that article[103]. Second, the text makes no mention whatsoever of the right to privacy, a notable omission given the scope of surveillance and censorship in the countries promoting the Code[104]. Thirdly, the 2015 Code reflects a reversal of emphasis between the rule, namely, the protection of freedom of expression, and the exception, the possibility of imposing restrictions on that freedom in limited circumstances: as explicitly clarified by the UN Human Rights Committee in its General Comment 34, such an inversion is inadmissible, since it puts in jeopardy the right itself[105].

In short, the centrality of sovereignty in the Sino-Russian conception of international law finds concrete expression in the cyber domain, where both Russia and China systematically restrict online rights and freedoms under broadly defined and often vague security justifications.

3.3. *Vague offences, weak human rights safeguards, extraterritorial reach: tracing the Sino-Russian stance on sovereignty primacy over human rights in the Cybercrime Convention*

Following the failure of the 2011 and 2015 Code of Conduct proposals, this approach resurfaced both in the text of the UN Cybercrime Convention and, even more explicitly, in the proposals put forward by Russia and China during its negotiation. This is reflected in three main sets of provisions: (a) the scope of offences that may be prosecuted under the Convention; (b) the limited human rights safeguards; and (c) the rules on jurisdiction. Together, these elements reveal how the Convention embodies the Sino-Russian idea of the interaction between sovereignty and protection of human rights. Applied to cyberspace, this understanding entails that States should exercise wide-ranging control over internet

[100] *Letter dated 2011/09/12*, cit., lett. f).
[101] See J. CARR, *Problems with China and Russia's International Code of Conduct for Information Security*, in *Digital Dao*, 22 September 2011, available at www.jeffreycarr.blogspot.com.
[102] *Letter dated 9 January 2015*, cit., n. 7.
[103] See S. MCKUNE, *An Analysis of the International Code of Conduct for Information Security: Will the SCO states' efforts to address "territorial disputes" in cyberspace determine the future of international human rights law?*, 28 September 2015, available at www.citizenlab.ca.
[104] Ibid.
[105] U.N. HUMAN RIGHTS COMMITTEE, General comment No. 34, *Article 19: Freedoms of opinion and expression*, U.N. Doc. CCPR/C/GC/34, 2011, para. 21.

governance, even where such control may conflict with the international human rights framework.

Starting with the first set of provisions, while the Budapest Convention focuses on cyber-dependent crimes, i.e., any crime that can only be committed using computers, computer networks or other forms of information communication technology[106], the Sino-Russian approach during the negotiations of the UN Cybercrime Convention has aimed to broaden the scope to include cyber-enabled crimes, i.e. crimes facilitated by the internet and digital technologies[107]. As highlighted by various NGOs, scholarship and the Office of the High Commissioner on Human Rights (OHCHR), this effort embodies a strategy by these States to incorporate into the Convention certain offences that, in their domestic legal systems, are frequently used to suppress online dissent[108]. For instance, China and Russia have pushed for the inclusion of offences such as dissemination of false information, digital data intended to mislead the user, and terrorism and extremism-related offences[109]. Even more revealingly, Russia has proposed a sweeping catch-all clause allowing States Parties to criminalize any other intentional act committed using information and communication technologies that causes significant damage[110]. In essence, the Sino-Russian approach has been to broaden the scope of the Convention, aiming for a degree of vagueness in the definition of the crimes falling within its application. Although not all of these proposals were ultimately incorporated into the final text, the underlying approach remained intact.

An example is article 4, which provides that «[i]n giving effect to other applicable United Nations conventions and protocols to which they are Parties, States Parties shall ensure that criminal offences established in accordance with such conventions and protocols are also considered criminal offences under domestic law when committed through the use of information and communications technology systems». This provision potentially extends the scope of the Convention to an unlimited number of crimes, which clearly conflicts with the principle of legality. Moreover, the Convention does not clarify whether «United Nations conventions and protocols» refers solely to treaties adopted within the UN framework or also includes bilateral agreements registered under Article 102 of the UN Charter. The problematic nature of Article 4 becomes even more evident when read in conjunction with Recital 5 of the Convention, which states that the AHC will continue its work with a view to adopting an additional protocol «addressing, inter alia, additional criminal offences as appropriate»[111]. This opens the door to a potential future expansion of the Convention's

---

106 C. MURPHY, *Understanding Cybercrime*, in *European Parliamentary Research Service* (EPRS), 2024, available at www.europarl.europa.eu, p. 2.

107 A. SUKUMAR and A. BASU, *Back to the territorial state: China and Russia's use of UN cybercrime negotiations*, cit., p. 273.

108 PRIVACY INTERNATIONAL AND ELECTRONIC FRONTIER FOUNDATION, *Privacy International and Electronic Frontier Foundation's Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty*, cit.; OFFICE OF THE HIGH COMMISSIONER ON HUMAN RIGHTS (OHCHR), *Human Rights and the Draft Cybercrime Convention*, cit., p. 3; F. SEATZU, *The New UN Convention on Cybercrime: Between Securing Cyberspace and Undermining Fundamental Rights and Freedoms*, cit., p. 238.

109 A. MARTIN, *China Proposes UN Treaty Criminalizes 'Dissemination of False Information*, in *The Record*, 17 January 2024, available at www.therecord.media. See also AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES, Sixth Session, *Draft Text of the Convention*, 1st September 2023, arts. 11, 15 *quinquies*, 15 *septies*,

110 *Draft Text of the Convention*, cit., art. 15 *undecies*.

111 *Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session*, cit., pp. 1-2.

scope via Article 4, effectively allowing the incorporation of new offences through reference to external legal instruments[112].

Secondly, by adopting vague definitions of criminal conducts and flexible requirements for intent, the Convention significantly broadens the range of conduct that may fall within its scope. In fact, Articles 7 and following obligate States Parties to criminalize certain behaviours that are often vaguely defined and need only be committed intentionally. The Convention leaves it up to individual States to decide whether to require an element of criminal or dishonest intent[113]. This has drawn significant criticism, with commentators warning that such vague and expansive provisions could be used to prosecute researchers or journalists whose intent is to hold governments accountable through investigative work[114].

Lastly, the problem of the indeterminacy of offences also arises in the provisions concerning the collection, preservation, and sharing of electronic evidence. Article 23, for example, extends the obligation to collect electronic evidence to «any criminal offence», without further limitation[115], while Article 35 requires States Parties to collect, obtain, preserve, and share electronic evidence in relation to «any serious crime». According to Article 2, a serious crime is defined as «a conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty». As a result, the scope of application of this provision is effectively determined by the domestic legal systems of the States Parties, which retain the discretion to define what constitutes a serious crime under their own legislation[116].

Turning to (b), China, but especially Russia, together with some like-minded States, pushed during the negotiations for a significant downsizing of human rights provisions[117]. First of all, this emerges from the debate on Article 6 of the Convention, which enshrines respect for human rights in the implementation of treaty obligations. Iran has put forward a proposal to delete the article altogether, while Russia has proposed to merge it with Article 24, which dictates conditions and safeguards[118]. Moreover, Moscow has voted against to the proposal to «take into consideration the special circumstances and needs of persons and groups in vulnerable situations in measures undertaken»[119] and to the inclusion of «the effective protection of human rights» among the measures included in art. 54 about technical assistance and capacity building[120]. China, for its part, voted against the inclusion of respect for international law among the safeguards required for managing personal data received from another State Party under the Convention[121].

With regard to the final text of the Convention, criticism has been raised concerning the literal wording of the provisions related to the protection of human rights[122]. Article 6,

---

112 OFFICE OF THE HIGH COMMISSIONER ON HUMAN RIGHTS (OHCHR), *Human Rights and the Draft Cybercrime Convention*, cit., p. 3.
113 *Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session*, cit., p. 3
114 A. ADAMS, D. PODAIR, *Confusion and Contradiction in the UN "Cybercrime" Convention*, in *Lawfare*, 9 December 2024, available at www.lawfaremedia.org.
115 *Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session*, cit., p. 3; see, in this respect, UNITED NATIONS SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF HUMAN RIGHTS WHILE COUNTERING TERRORISM B. SAUL, *Human Rights Assessment of the Draft United Nations Cybercrime Convention*, cit.
116 *Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session*, cit., p. 3.
117 A. SUKUMAR, A. BASU, *Back to the territorial state: China and Russia's use of UN cybercrime negotiations*, cit., p. 274.
118 *Draft Text of the Convention*, cit., art. 5.
119 Ibid., art. 5, para. 2.
120 Ibid., art. 54, lett. i bis).
121 Ibid. art. 36, para. 2.
122 See M.M. TENNIS, *A United Nations Convention on Cybercrime*, in *Capital University Law Review*, 2020, p. 189 ff.

paragraph 1, for example, states that «States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law». Similarly, Article 24 provides that «each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate the principle of proportionality». The issues with these provisions are twofold.

First, the provisions delegate the definition and implementation of conditions and safeguards entirely to domestic legal systems, requiring only that they comply with general human rights and proportionality principles, an expectation that, as illustrated by the Russian and Chinese legal frameworks on information security, may not be realistically met[123]. Second, no monitoring mechanism has been established to ensure compliance with human rights in the implementation of the Convention's provisions. This absence leaves room for restrictive and instrumental interpretations, particularly by autocratic regimes, which may exploit the vague wording of the Convention for repressive purposes. This is unlike, for example, the Budapest Convention, which, although it does not establish formal oversight committees, provides for meetings among the Parties and technical cooperation mechanisms designed to review how States implement its provisions[124].

What is perhaps even more troubling is what the Convention leaves out. Nowhere does it clearly affirm key principles such as legality and necessity, which should underpin any exercise of State power in the criminal justice context[125]. As underlined by the OHCHR, there is also no mention of requiring prior judicial review before procedural powers are used, nor are there meaningful constraints on how far these powers can extend or how long they can be applied. Individuals or entities affected by such measures are not guaranteed timely notification or access to information about the actions taken against them, raising serious transparency concerns. Furthermore, those who may suffer harm as a result are not clearly granted access to effective remedies. The Convention is also silent on the need to respect the confidentiality of communications that are legally protected, such as those between lawyers and their clients[126].

Lastly, another embodiment of this sovereignty-centered approach to human rights in the UN Cybercrime Convention lies in the provisions that potentially infringe on the right to privacy[127]. Indeed, on the one hand, a number of provisions grant extremely broad governmental powers over digital data without adequate safeguards; on the other hand, certain provisions could push internet service providers to exercise extensive surveillance powers or to grant access to encrypted information.

---

123 A. ADAMS, D. PODAIR, *Confusion and Contradiction in the UN "Cybercrime" Convention*, cit.; K. RODRIGUEZ, *The UN General Assembly and the Fight Against the Cybercrime Treaty*, in *Electronic Frontier Foundation*, 26 September 2024, available at www.eff.org.; F. SEATZU, *The New UN Convention on Cybercrime: Between Securing Cyberspace and Undermining Fundamental Rights and Freedoms*, cit., pp. 232-233.

124 F. SEATZU, *The New UN Convention on Cybercrime: Between Securing Cyberspace and Undermining Fundamental Rights and Freedoms*, cit., pp. 231-232.

125 *Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session*, cit., p. 2.

126 OFFICE OF THE HIGH COMMISSIONER ON HUMAN RIGHTS (OHCHR), *Human Rights and the Draft Cybercrime Convention*, cit., p. 9.

127 See PRIVACY INTERNATIONAL, *Privacy International's Comments on the Revised Draft Text of the UN Cybercrime Convention* (November 2023), available at www.unodc.org; F. SEATZU, *The New UN Convention on Cybercrime: Between Securing Cyberspace and Undermining Fundamental Rights and Freedoms*, cit., p. 236.

Article 28 offers the clearest illustration of the first dynamic, empowering national authorities to penetrate computer systems and the data they contain. Notably, paragraph 4 of this article allows officials to compel any private actor (whether an internet service provider, a platform operator, a systems administrator, or even an ordinary user with pertinent credentials) to furnish whatever information is needed to make that access possible. Such powers could give governments sweeping insight into personal communications and other sensitive data, posing a serious risk of disproportionate intrusions into privacy. They might even enable the alteration or manipulation of the content of those exchanges, raising alarms about potential curbs on freedom of expression and knock-on effects for other fundamental rights[128].

As for the role of internet service providers, Russia initially proposed the adoption of a code of conduct to regulate their activities[129], while China suggested obliging them to take adequate measures to respond to criminal activities[130]. During the discussion on the final draft, this evolved into a proposal to include an obligation to criminalize the "unlawful provision of services", defined as any digitally-enabled service provided intentionally and without right[131]. The acceptance of such a provision would have inevitably granted States wide discretion in determining what constitutes the intent of an internet service provider, raising serious concerns, particularly in light of the practices of countries like China and Russia, where such discretion could be used to justify broad repression and control over digital services[132].

While these proposals were ultimately excluded from the final text of the Convention, their underlying values reemerged in other provisions. A notable example is article 18, which requires States «to establish the liability of legal persons for participation in the offences established in accordance with this Convention», without requiring any element of intent. This broad formulation likely means that internet service providers, in order to avoid any potential liability, will be compelled to exercise pervasive monitoring over content, effectively resulting in a violation of users' right to privacy and freedom of expression[133]; in the same vein, Articles 29 and 30 oblige each State to empower its competent authorities to «[c]ompel a service provider, within its existing technical capability: (i) To collect or record, through the application of technical means in the territory of that State Party; or (ii) To cooperate and assist the competent authorities in the collection or recording of» traffic data and content data in real time, respectively. In short, whether through the threat of liability or through direct coercion by the authorities, internet service providers risk becoming tools for significant governmental interference with users' right to privacy[134].

---

128 Ibid., p. 7

129 RUSSIAN FEDERATION, *Russian proposal in (UNODC) United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, 2021, art. 43, available at www.unodc.org

130 PEOPLE'S REPUBLIC OF CHINA, *China Suggestions on the Scopes, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes*, 2022, n. 2, available at www.unodc.org.

131 *Draft Text of the Convention*, cit., art. 10 *ter*.

132 A. SUKUMAR, A. BASU, *Back to the territorial state: China and Russia's use of UN cybercrime negotiations*, cit., p. 275.

133 OFFICE OF THE HIGH COMMISSIONER ON HUMAN RIGHTS (OHCHR), *Human Rights and the Draft Cybercrime Convention*, cit., p. 6 and F. SEATZU, *The New UN Convention on Cybercrime: Between Securing Cyberspace and Undermining Fundamental Rights and Freedoms*, cit., p. 237.

134 It is no coincidence that the private stakeholders invited to take part in the treaty drafting process criticized it, warning that it could become "a pretext for non-democratic regimes to further threaten the free and open internet by sealing off their digital borders", MICROSOFT, *Submission to the First Session on the Upcoming Negotiations on a Possible Cybercrime Convention*, 1 March 2022, available at www.unodc.org.

Lastly, moving on to point (c), the last set of provisions concerns the exercise of jurisdiction. During the negotiations, Sino-Russian proposals sought to incorporate into the Convention the criterion of jurisdiction based on the effects of conduct. According to these proposals, a State would have jurisdiction over crimes falling within the Convention's scope, *inter alia*, even when «[t]he offence is committed wholly or partly outside the territory of [a] State Party but its effects in the territory of that State Party constitute an offence or result in the commission of an offence»[135], or when the «offence is committed against the State Party»[136]. More generally, jurisdiction would thus be determined by «giving priority to where the consequences of criminal activity occur»[137]. The expansion of jurisdiction as outlined in the Chinese and Russian proposals was accompanied by other proposals from these States aimed at limiting the grounds for refusing to provide mutual assistance, in particular by preventing States from refusing requests for mutual legal assistance on the basis of the political nature of the offences prosecuted, or those motivated by a person's sex, race, language, religion, nationality, ethnic origin or political opinions[138].

These provisions were ultimately not included in the final text of the Convention. However, the underlying intent, namely, the extension of State jurisdiction beyond territorial boundaries, resurfaces in the passive personality provision found in Article 22, paragraph 2, subparagraph (a): «a State Party may also establish its jurisdiction […] when: a) The offence is committed against a national of that State Party». Scholars have pointed out that, within the broader context of the Convention, the expansive potential of this rule has been underestimated[139]. It has been observed that this provision enables a State to prosecute a foreign national who has committed an offence in another State's territory, solely on the basis that the conduct affected one of its own citizens[140]. To illustrate this point, an author give the example that «Russia could seek Turkey's help in surveilling and extraditing an American journalist vacationing in Istanbul who discovered a misconfigured database and reported on the exposure of Russian citizens' personal data»[141]. This scenario becomes even more concerning in light of the Convention's weak human rights safeguards, which would be the only possible protection available to the American journalist in the example.

In conclusion, the Convention's vague definition of offences, the inclusion of cyber-enabled crimes, the inadequate protection of human rights, and the broad expansion of jurisdiction collectively portray a vision of cyberspace marked by the pervasive and intrusive reach of State power. As this analysis has shown, the Convention reflects a key dimension of the Sino-Russian conception of international law, one in which the primacy of State sovereignty is affirmed at the expense of the protection of fundamental rights. Far from being a neutral instrument of global cybercrime governance, it constitutes a rearticulation of earlier proposals for cybersecurity regulation advanced in 2011 and 2015.

---

135 *Draft Text of the Convention*, cit., art. 22, para. 2, lett. c) *bis*.
136 Ibid., art. 22, para. 2, lett. d).
137 PEOPLE'S REPUBLIC OF CHINA, *China Suggestions on the Scopes, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes*, cit., p. 5, n. 7.
138 *Draft Text of the Convention*, cit., art. 40, para. 21, lett. c *bis*) and c *ter*).
139 E. SCHER-ZAGIER, *The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize*, cit.
140 See E. SCHER-ZAGIER, *Jurisdictional Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdiction*, in *Yale Journal of Law and Technology*, forthcoming, 2024.
141 E. SCHER-ZAGIER, *The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize*, cit.

4. *The concern to limit Western dominance in cyberspace and to criminalize cyber operations: mirroring non-interference in the internal affairs of other States*

4.1. *The principle of non-interference in the internal affairs of others States in the Sino-Russian approach to international law*

A final important corollary of the concept of sovereignty in the Sino-Russian approach is the principle of non-interference in the internal affairs of other States. This principle plays a central role in the present discussion, as it reflects the external dimension of sovereignty, i.e. independence from external forces[142], which is especially significant in the Sino-Russian conception of international law due to historical factors[143].

As for China, this emphasis stems from the historical trauma that is referred to as the "century of humiliation", which culminated in the imposition of the so-called "unequal treaties" by Western powers following the Opium Wars[144]. These treaties are seen as emblematic of foreign interference in China's sovereignty, and the period that followed is interpreted as a gradual reassertion of national identity and a slow reclamation of full Chinese sovereignty[145]. However, this sovereignty is perceived as continuously threatened by attempts, especially by European countries and the United States, to apply their laws extraterritorially[146]. Consequently, China regularly invokes the imperialism and hegemonism as threats to its sovereignty and, in line with this narrative, strongly reaffirms the principle of non-interference as a cornerstone of international law[147].

Though rooted in a different historical trajectory, Russia shares a similar insistence on non-interference. As discussed in the previous paragraph, Russia invokes internal sovereignty as a limit to the application of human rights norms. The same logic is applied to external sovereignty, which is used to argue against foreign involvement in domestic matters, particularly under the banner of human rights[148]. Most frequently, this principle is cited in the context of rejecting the legitimacy of unilateral sanctions: they are portrayed in Russian rhetoric as illegitimate interference in the internal affairs of the Russian Federation[149]. Once again, the primary targets of this critique are Western States, accused of legal imperialism and

142 In this regard, see Individual Opinion by M. Anzilotti, in Permanent Court of International Justice, *Customs Regime between Germany and Austria*, Advisory Opinion of 5 September 1931, *Series A/B, No. 41*, p. 57.
143 T. WANG, *International Law in China: historical and contemporary perspectives*, cit., p. 296 ff.
144 P. C. W. CHAN, *China, State Sovereignty and International Legal Order*, Leiden, 2015; S. CHESTERMAN, *Asia's Ambivalence About International Law and Institutions: Past, Present and Futures*, in *European Journal of International Law*, 2016, p. 951 ff.
145 H. XUE, *Chinese Contemporary Perspectives on International Law*, cit., p. 90 ff.
146 A. ROBERTS and M. KOSKENNIEMI, *Is International Law International?*, cit., p. 295 ff.
147 PEOPLE'S REPUBLIC OF CHINA OFFICE OF STATE COUNCIL, *China's National Defence in 2000*, 2000, available at www.china.org.cn.; Statement by WEN JIABAO, Premier of the State Council of the People's Republic of China, *A China Committed to Reform and Opening-up and Peaceful Development*, at the General Debate of the 63rd Session of the United Nations General Assembly on 24 September 2008; Y. WANG, *China: A Staunch Defender and Builder of International Rule of Law*, cit., p. 637.
148 A. ROBERTS and M. KOSKENNIEMI, *Is International Law International?*, cit., p. 295.
149 MINISTRY OF FOREIGN AFFAIRS OF RUSSIAN FEDERATION, *Concept of the Foreign Policy of the Russian Federation*, cit., para. 31; PERMANENT MISSION OF THE RUSSIAN FEDERATION TO THE UNITED NATIONS, *Statement by First Deputy Permanent Representative Dmitry Polyanskiy at UNSC open debate "General issues relating to sanctions: preventing their humanitarian and unintended consequences"*, 7 February 2022, available at www.russiaun.ru; PERMANENT MISSION OF THE RUSSIAN FEDERATION TO THE UNITED NATIONS, *Statement by Permanent Representative Vassily Nebenzia at an informal Arria Formula meeting on Humanitarian Impact of Unilateral Coercive Measures*, 25 November 2024, available at www.russiaun.ru.

hegemonic practices. Thus, despite their distinct historical and political backgrounds, Russia and China converge entirely in their shared emphasis on non-interference as a key corollary of sovereignty.

Indeed, the principle of non-interference features prominently in the sources they frequently reference, as well as in their Joint Statements on international law. Among the former, the Five Principles of Peaceful Coexistence explicitly include non-interference as a core tenet. Likewise, the Charter of the United Nations enshrines this principle in Article 2(7), which limits the authority of the UN in matters essentially within the domestic jurisdiction of any State, thereby affirming the reserved domain of State sovereignty. Lastly, the Declaration on Principles of International Law concerning Friendly Relations reaffirms the duty of all States to refrain from intervening, directly or indirectly, in the internal or external affairs of other States[150].

As for their Joint Statements on international law, China and Russia express an even clearer and more explicit commitment to the principle of non-intervention. They jointly affirm that they «fully support the principle of non-intervention in the internal or external affairs of States, and condemn as a violation of this principle any interference by States in the internal affairs of other States, in particular when undertaken with the aim of forging change of legitimate governments», therefore they «condemn extraterritorial application of national law by States not in conformity with international law as another example of violation of the principle of non-intervention in the internal affairs of States» [151]. In the same vein, they «oppose and condemn unilateral sanctions that violate international law, in particular the principles of sovereign equality of States, State immunity and non-interference in internal affairs of States, and are not authorized by the Security Council, as well as long-arm jurisdiction and division along ideological lines, and emphasize that States have the right to conduct normal economic and trade cooperation»[152]. A natural corollary to this conception of non-interference is a firm condemnation of the unilateral use of force, in violation of the prohibition enshrined in the UN Charter, and thus not carried out in legitimate self-defense. This principle is consistently reaffirmed in all Joint Statements[153] and has been interpreted in academic literature as a critical reference to the unilateral interventions conducted by Western States in Kosovo and Iraq. It also underpins a broader denunciation of the "double standards" whereby such States call to respect international law only when aggressive policies are perpetrated by Russia or China[154].

However, despite their strong emphasis on the principle of non-interference as a core expression of sovereignty, both China, and especially Russia, adopt a different stance to the sovereignty of their neighbours. Russia has developed the concept of a "near abroad", effectively extending its notion of sovereignty to include former Soviet republics, as illustrated by its relationship with Ukraine and Georgia[155]. China, while not advancing a similar doctrine, seems to interpret regional cooperation in ways that suggest a broader

---

150 *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States*, cit., p. 123.
151 2016 Joint Declaration, para. 4 and 2025 Joint Declaration, para. 9; See also 2021 Joint Statement, n. III and 2022 Joint Statement, n. III.
152 2025 Joint Declaration, para. 8; see also 2016 Joint Declaration, para. 6; 2021 Joint Statement, n. IV and 2022 Joint Statement, n. IV.
153 2016 Joint Declaration, para. 3; 2021 Joint Statement, n. III ; 2022 Joint Statement, n. III; 2025 Joint Declaration, para. 6.
154 A. ROBERTS and M. KOSKENNIEMI, *Is International Law International?*, cit., p. 295.
155 E. GÖTZ, *Near Abroad: Russia's Role in Post-Soviet Eurasia* in *Europe-Asia Studies*, 2022, p. 1529 ff.

notion of sovereignty[156]. This is particularly evident in the South China Sea, where its actions point to a vision of regional order that goes beyond simple coexistence[157]. In both cases, the principle of non-interference appears to apply mainly to actors from outside the region, those with different historical, cultural, and political backgrounds, whereas regional powers like China and Russia claim a legitimate role in shaping their immediate environment[158]. This view is reflected in the importance both countries place on regional cooperation, often presented as an expression of sovereign equality within a multipolar world[159]. In this regard, particularly explicit is the 2021 Joint Statement, in which Russia and China declare that they «stand against attempts by external forces to undermine security and stability in their *common adjacent regions*, intend to counter interference by outside forces in the internal affairs of sovereign countries under any pretext, oppose colour revolutions, and will increase cooperation in the aforementioned areas»[160].

Ultimately, the Sino-Russian emphasis on the principle of non-interference reflects a broader critique of what they perceive as Western attempts to dominate and monopolize international relations. In contrast, they assert the need to preserve inviolable spheres of national sovereignty, pushing back against what they view as an overreach into the internal affairs of sovereign States[161]. This stance is often closely linked to the principle of sovereign equality, which, as explained above, underlines the idea that all States, regardless of their power or influence, should be treated as equals in the international system[162].

4.2. *Non-Interference in Sino-Russian cybersecurity practice: the "sovereignization" of the internet as a response to foreign cyber threats*

This perspective on non-interference extends seamlessly into the Sino-Russian approach to cybersecurity. Both countries have been at the forefront of advocating for what they term "cybersovereignty", i.e. a model of digital governance rooted in national control over information infrastructure, aimed at limiting what they see as Western, especially American, dominance in cyberspace. This agenda rests on three main pillars: a critique of U.S. technological hegemony, a broad and preemptive definition of cyber threats, including the development of *potentially* offensive tools that might hinder sovereign spaces; and, in turn, the perceived need for the "sovereignization" of the internet, whereby all physical infrastructure should be located entirely within the borders of the State.

Consistent with this perspective, Russia has pursued a strategy to assert sovereign control over its digital infrastructure. Commonly referred to as the "sovereignization" of the internet, this effort seeks to create an autonomous national segment by ensuring that all

156 In this respect, see MINISTRY OF FOREIGN AFFAIRS OF THE POPULAR'S REPUBLIC OF CHINA, *Outlook on China's Foreign Policy on Its Neighborhood In the New Era*, 24 october 2023, available at www.mfa.gov.cn.
157 For the Chinese position, see MINISTRY OF FOREIGN AFFAIRS OF THE POPULAR'S REPUBLIC OF CHINA, *China Stays Committed to Peace, Stability and Order in The South China Sea*, 23 March 2022, available at www.mfa.gov.cn.
158 A. ROBERTS and M. KOSKENNIEMI, *Is International Law International?*, cit., p. 292.
159 C. J. FUNG, *Global South Solidarity? China, Regional Organisations and Intervention in the Libyan and Syrian Civil Wars*, in *Third World Quarterly*, 2016, p. 33 ff. and L. KHASANOVA, A. SIMONYAN, *(Geo)politicizing International Law of Cyberspace in Post-Soviet Eurasia*, cit.
160 2021 Joint Statement, n. III.
161 L. MÄLKSOO, *Russia and China Challenge the Western Hegemony in the Interpretation of International Law*, cit.
162 Ibid.

critical hardware is located within Russian territory. The goal is to shield the domestic digital space from external interference by reducing dependence on global networks seen as under U.S. influence[163].

As for China, it advanced the *Global Initiative on Data Security* at the UN General Assembly in 2020[164]. The initiative calls for the responsible use of ICTs, emphasizing non-interference, respect for sovereignty, and the protection of critical infrastructure and sensitive data. It explicitly opposes practices such as cyber intrusions and unauthorized data collection that violate national jurisdictions or threaten State security[165]. In line with this external threat perception, China has also reinforced its domestic legal framework: the 2021 *Data Security Law* imposes obligations on operators to safeguard key digital infrastructure from foreign risks[166], while the 2023 amendment to the *Counter-Espionage Law* broadened its scope to include acts of cyber espionage targeting China's information systems[167].

As for their joint initiatives, the 2009 SCO Agreement on Cooperation in the Field of Information Security captures this view by identifying among the six major threats to information security «the use of a dominant position in the information space to the detriment of the interest and security of other States»[168], explaining that this threat «is caused by the unevenness in the development of information technologies in different countries and the current trend of the increased "digital gap" between developed and developing countries. Some States that have advanced in the development of information technologies deliberately hinder the development of other countries and their access to information technologies creating serious danger for countries with insufficient information capacity»[169]. The concern extends beyond mere access: it includes the presence of concealed functionalities in exported software and hardware, which could enable surveillance or manipulation of another State's systems[170]. This threat is closely connected to another identified in Article 2: the «development and use of information weapons, as well as the preparation and conduct of information warfare». As outlined in Annex 2, this danger stems from the mere creation and advancement of such weapons, which are seen as posing an immediate risk to the critical

163 A. SHCHERBOVIC, *Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the "Sovereignization" of the Internet in Russia*, in L. BELLI (ed.), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*, cit., p. 68.

164 Note by Secretary General, Developments in the field of information and telecommunications in the context of international security, 1 August 2023, UN Doc. A/78/265, the full text is available at www.documents.unoda.org.

165 This act falls within the broader framework of China's Global Security Initiative, on which see Y. WANG, State Councilor and Minister of Foreign Affairs, *Acting on the Global Security Initiative to Safeguard World Peace and Tranquility*, 24 April 2022, available at www.fmprc.gov.cn; MINISTRY OF FOREIGN AFFAIRS OF THE PEOPLE'S REPUBLIC OF CHINA, *Jointly Implementing the Global Security Initiative For Lasting Peace and Security of the World*, 31 October 2023, available at www.mfa.gov.cn; C. XIAODONG, Vice Minister of Foreign Affairs of the People's Republic of China, *Jointly Acting on the Global Security Initiative and Building a Community with a Shared Future for Mankind that Enjoys Universal Security*, Keynote Speech At the 11th Beijing Xiangshan Forum, 15 September 2024, available at www.mfa.gov.cn and

166 Data Security Law of the People's Republic of China, 2021, whose English translation is available at www.chinalawtranslate.com.

167 Counter-espionage Law of the People's Republic of China, 2023, whose English translation is available at www.chinalawtranslate.com.

168 Article 2 of the Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization.

169 Annex 2 of the 2009 Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, n. 4.

170 Ibid.

infrastructure of States. This phenomenon is regarded as a primary threat to information security, with the potential to trigger a new arms race in the digital domain[171].

For this reason, Article 3 of the agreement commits States to cooperate in the development of international legal norms designed to address these emerging challenges. In pursuit of this objective, several SCO member States incorporated a corresponding set of principles into the two Codes of Conduct submitted to the United Nations in 2011 and 2015. Both documents articulate a clear commitment to refraining from the use of information and communication technologies as instruments of interference in the internal affairs of other countries, particularly when such actions threaten their political, economic, or social stability.[172] Equally central is the emphasis they place on securing ICT supply chains, with the aim of preventing technologically dominant actors from leveraging their position to restrict other States' capacity to manage their digital environments autonomously[173]. More broadly, the texts reaffirm the right and responsibility of States to protect their information space and critical infrastructure from threats, sabotage, and attacks, and call for restraint in the use of ICTs for hostile purposes, including acts of aggression or activities that endanger international peace and security[174]. Finally, they underscore the need to prevent the proliferation of information weapons and related technologies[175].

These two dimensions, i.e. the notion that the principal threats to information security arise from technological dominance and the development of information weapons, can be interpreted as an implicit reference to the United States and the major technology firms based within its jurisdiction: through their significant influence over the global digital landscape, they are perceived as key actors contributing to the materialization of these risks[176].

However, not only the 2011 and 2015 Codes of Conduct were not adopted, but also the outcomes of the GGE and UN GGE on these aspects were considered mostly unsatisfying by China and Russia. Although the 2015 GGE report marked a partial recognition of the risks posed by cyber operations targeting critical infrastructure, urging States not to conduct or knowingly support activities that intentionally damage or impair such systems[177], it simultaneously limited this obligation to operations that exceed the threshold of the use of force. This narrow interpretation excluded a wide range of disruptive activities, such as cyber espionage and sabotage, that fall below that threshold. The 2021 report reaffirmed this restrictive scope, confirming that the commitment did not extend to sub-threshold operations[178], thus failing to address the broader spectrum of foreign interference that states like Russia and China had repeatedly denounced.

This limitation reflected again a fundamental divide between competing visions of international cyber governance. For Russia and China, these forms of interference were not merely security threats but direct challenges to their sovereignty and internal stability, particularly given the dominance of Western technological powers. In contrast, Western

171 Ibid.
172 *Letter dated 9 January 2015*, cit., n. 3.
173 *Letter dated 9 January 2015*, cit., n. 5. *Letter dated 2011/09/12*, cit., lett. d).
174 *Letter dated 9 January 2015*, cit., n. 2; *Letter dated 2011/09/12*, cit., lett. b).
175 *Letter dated 9 January 2015*, cit., n. 6. *Letter dated 2011/09/12*, cit., lett. b).
176 on this issue, see K. POLLPETER, *Chinese writings on cyberwarfare and coercion*, in J.R. LINDSAY, T.M. CHEUNG, D. REVERON (eds.), *China and Cybersecurity: Espionage, strategy and politics in the digital domain*, Oxford, 2015, p. 147.
177 UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015, UN Doc. A/70/174.
178 UNGA, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyber-space in the Context of International Security*, 14 June 2021, UN Doc. A/76/135.

States have traditionally focused on cyber threats primarily in terms of their potential to cause physical damage or disrupt critical infrastructure[179].

4.3. *Non-interference in the UN Cybercrime Convention: defending critical information infrastructure through criminalization*

The Sino-Russian response has been to pursue alternative legal avenues, most notably within the negotiations for the UN Cybercrime Convention. There, both States sought to institutionalize a broader conception of unlawful interference, moving beyond kinetic thresholds and toward the protection of digital sovereignty.

Russia pushed for the inclusion of a broadly defined offense of "unlawful interference" with critical infrastructure, extending even to the creation of software capable of impeding or accessing information systems[180]. China similarly proposed criminalizing the intrusion into or destruction of ICT systems and data, grounding these efforts in its broader conception of the principle of non-interference and the sovereign equality of States[181]. Together, they argued for an "equal right" of all States to defend their critical information infrastructure against misuse or unauthorized access[182].

Particularly revealing were the provisions proposed around cyber espionage. China advocated for the prohibition of data collection "by States" through technical means that circumvent network protections, when such conduct contravenes the domestic laws of the target state[183]. Russia, for its part, sought to criminalize the interception of data traffic not intended for public use[184]. In both cases, the goal was clear: to challenge what they perceived as a permissive international legal environment that enables Western intelligence operations under the guise of lawful State practices.

These proposals were met with firm resistance from the United States and several European States, which preferred a narrower interpretation of cybercrime focused on clearly harmful conduct such as the physical destruction of infrastructure[185].

Although the final version of the treaty did not explicitly address cyber espionage or critical infrastructure, the inclusion of general offenses such as illegal access, interception,

---

179 A. SUKUMAR, A. BASU, *Back to the territorial state: China and Russia's use of UN cybercrime negotiations*, cit., p. 271.
180 RUSSIAN FEDERATION, *Russian proposal in (UNODC) United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, cit., art. 10 *bis*.
181 PEOPLE'S REPUBLIC OF CHINA, *China Suggestions on the Scopes, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes*, cit., art. 3 (1).
182 RUSSIAN FEDERATION also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan, available at www.unodc.org, Art. 46 (5).
183 PEOPLE'S REPUBLIC OF CHINA, *China Suggestions on the Scopes, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes*, cit., art. 4(1).
184 RUSSIAN FEDERATION, *Russian proposal in (UNODC) United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, cit., art. 7.
185 See, among others, AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES, *Consolidated Negotiating Document on the Preamble, the Provisions on International Cooperation, Preventive Measures, Technical Assistance and the Mechanism of Implementation and the Final Provisions of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, Fifth Session, 21 April 2023, available at www.unodc.org and EUROPEAN UNION EXTERNAL ACTION, *EU Statement – UN Ad-Hoc Committee for a UN Convention on Cybercrime: Objectives and Scope of the Convention and EEAS*, 2022, available at www.eeas.europa.eu.

and interference may still leave room for broader interpretations aligned with Sino-Russian concerns[186].

In this regard, it is worth noting a final element of complexity: the ambivalent interpretation of the principle of non-interference, which, as previously observed, tends to be applied asymmetrically by China and Russia. While both States actively promote international norms aimed at criminalizing foreign cyber interference, often invoking the need to safeguard their sovereignty, they adopt a more flexible stance when it comes to their own actions[187]. Russia, in particular, has been repeatedly identified as one of the most active countries in conducting cyber operations abroad, frequently through proxies or private actors[188]. This seemingly contradictory behaviour becomes more intelligible when placed in the broader context of their conception of sovereignty, which distinguishes sharply between their own entitlement to act in defense of national interests and the illegitimacy of similar conduct by others. Framed in this way, their advocacy for stricter legal prohibitions on interference aligns with a broader critique of Western double standards[189]: while denouncing U.S. and allied cyber activities as violations of international norms, they implicitly assert a special status for themselves in the governance of cyberspace[190].

5. *Conclusion*

In conclusion, through their domestic legal systems, diplomatic practice, and Joint Statements, Russia and China have progressively articulated a distinctive vision of international law, that places the principle of sovereignty at its core. In the Sino-Russian understanding, this principle entails three key corollaries: internally, the primacy of State interests over the protection of individual rights; externally, the sovereign equality of States and the principle of non-interference in their domestic affairs. Such a vision is consistently framed through frequent references to the Five Principles of Peaceful Coexistence and a strict adherence to the principles enshrined in the UN Charter, as well as to the 1970 Declaration on Principles of International Law concerning Friendly Relations. The resulting normative framework amounts to an implicit, and at times explicit, critique of what Russia and China perceive as a distortion of international legal norms by Western powers, particularly the United States, and of the double standards with which those norms are applied. As a counter to this perceived imbalance, Moscow and Beijing have championed the emergence of a genuinely multipolar international legal order, rooted in a return to the principle of sovereignty.

The initial arena for this alternative legal project has been cyberspace, as a domain where international law remains underdeveloped and contested. Faithful to their conception of sovereign equality, and to its corollary of equal participation in international lawmaking, China and Russia have shown unprecedented activism in United Nations fora dedicated to

[186] *Cybercrime Convention*, cit., articles 7, 8, 9 and 10.
[187] E. KORZAK, *Russia's Cyber Policy Efforts in the United Nations*, *Tallinn Paper No.11, NATO Cooperative Cyber Defence Centre of Excellence*, 2021, available at www.ccdcoe.org.
[188] J. HAKALA, J. MELNYCHUK, *Russia's Strategy in Cyberspace, in NATO Strategic Communications Centre of Excellence*, 2021, available at www.stratcomcoe.org.
[189] MINISTRY OF FOREIGN AFFAIRS OF THE PEOPLE'S REPUBLIC OF CHINA, *Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference,* 12 April 2023, available at www.mfa.gov.cn.
[190] C. CAI., *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously*, Oxford, 2019, p. 160.

cybersecurity. There, they have sought to resist the wholesale application of existing international norms, seen as a reflection of the "old order", and have instead promoted the development of new rules grounded in their normative preferences. With limited success in shaping the cybersecurity agenda, they have shifted their focus to the negotiations of the UN Cybercrime Convention, adopted in 2024.

Both the proposals advanced by Russia and China during the negotiation of the Convention and, in some instances, the Convention's final provisions, reflect the key corollaries of the principle of sovereignty as understood within the Sino-Russian stance on international law. With regard to the internal dimension of sovereignty, the notion of the State as the supreme authority over all matters within its borders has materialized in broad and ambiguously worded provisions, which confer extensive criminalization powers upon national authorities. These include vaguely defined scopes of application and offences, minimal human rights safeguards, and the possibility for States to assert extraterritorial jurisdiction over acts allegedly producing effects within their territory, even if committed entirely abroad. As for the external dimension, the desire to limit U.S. dominance in cyberspace and to preserve domestic informational autonomy, invoked under the principle of non-interference, has driven efforts to criminalize foreign acts perceived as intrusive. As previously discussed, this includes conduct that does not meet the threshold of the use of force, yet is viewed as compromising the integrity of a State's information environment, such as cyber espionage, unauthorized data extraction, or intrusions into critical infrastructure.

This alternative vision of international law, and the attempt to enshrine it in the legal regulation of cyberspace and cybercrime, has met firm opposition from the United States and the so-called "like-minded" States. These actors have largely rejected the need for new norms, favoring instead the application of existing international law to cyberspace. They advocate a liberal cyber order based on a multistakeholder model of governance, i.e. one that distributes authority across governments, private actors, and civil society, rather than the State-centric approach promoted by Russia and China.

More broadly, the evolution of legal frameworks in the fields of cybersecurity and cybercrime serves as a particularly revealing case for observing how competing visions of international law are negotiated, challenged, and asserted. It is, in many ways, the testing ground for what could become a broader paradigm shift, one whose implications may well reverberate across other domains of international legal regulation.