ILGSPD Publication Series
No 3/24: Background Paper

The Open-Ended Working Group on Information and Communication Technologies: How do Russia and China define gaps in existing international law?

Chloe Young
May 2024

ERASMUS MUNDUS JOINT MASTER
International Law of Global Security, Peace and Development

Erasmus Mundus Joint Master in International Law of Global Security, Peace and Development

International Law of Global Security, Peace and Development (ILGSPD) is a multidisciplinary Master's degree delivered collaboratively by an international consortium composed of six Higher Education institutions: University of Glasgow, Institut Barcelona d'Estudis Internacionals, University of Tartu, Leuphana University of Luneburg, Radboud University, and Université libre de Bruxelles. It is recognised and funded by the European Commission as an Erasmus Mundus Joint Master Degree (EMJMD). The programme provides the next generation of lawyers and policy makers with expert knowledge required to respond to pressing challenges of global security, peace and development and trains tomorrow's leaders to navigate the political context of international law.

ILGSPD Publication Series

ILGSPD Publication Series aims to showcase the work developed by the programme's postgraduate students, in the form of a dissertation, working paper, or policy brief. Publications address themes of global security, peace and development, broadly understood, through the lens of international law, international relations, and/or sustainability.

Series Editor: Dr Asli Ozcelik Olcay

Coordinating Institution:
University of Glasgow
University Avenue
Glasgow G12 8QQ
Scotland, United Kingdom
E-mail: ilgspd@glasgow.ac.uk
www.globalsecuritylaw-erasmusmundus.eu

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of contents

The Open-Ended Working Group on Information and Communication Technologies: How do Russia and China define gaps in existing international law?

Chloe Young[*]

Introduction

In 2013, States agreed that international law, in particular the United Nations (UN) Charter, is applicable and essential in cyberspace.[1] In subsequent discussions within the Groups of Governmental Experts (GGEs) and Open-Ended Working Groups (OEWGs), States have reaffirmed international law's applicability in cyberspace. However, the current OEWG (2021-2025) on security of and in the use of information and communications technologies (ICTs) is at a crossroads. One group of States argues existing international law can and should be applied in cyberspace. Another group of States, including Russia and China, supports the creation of a new legally binding instrument setting out international legal principles for cyberspace due to alleged gaps in existing international law. In taking this discussion forward, it is important to understand how Russia and China perceive 'gaps' in existing international law.

A review of numerous government statements and OEWG session recordings reveals that Russia and China see gaps in existing international law mainly in the following areas: qualification of computer attacks as armed attacks, attribution of malicious cyber activity, definition of illegal cyber behaviour, assigning responsibility to manufacturers for the safe production of new products, countering online terrorist activity, and addressing the dissemination of illegal online content. Despite identifying these alleged gaps, Russia and China affirm that the following international legal principles apply in cyberspace: sovereignty, non-interference in internal affairs, the peaceful settlement of disputes, and the inadmissibility of unsubstantiated accusations against states for wrongful acts with ICTs. One recent notable shift in Russia's position was its acknowledgment that human rights should be addressed within the OEWG. However, Russia has consistently argued that international humanitarian law (IHL) cannot be applied in cyberspace and avoided explicitly mentioning the principle of state responsibility.

---

[*] Chloe Young currently studies towards the Erasmus Mundus Joint Master's Degree in International Law of Global Security, Peace and Development pursuing a specialisation in International Law and Human Rights. She holds a BA in Politics and Chinese from Whitman College located in Washington, USA. Contact emails: 2792430y@student.gla.ac.uk and youngchloemarie@gmail.com

[1] UNGA 'Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98.

Although China's rhetoric is more cautious than Russia's, the country still argues that international humanitarian law legitimizes cyber conflicts and cannot be endorsed in cyberspace. Unlike Russia, China explicitly holds that the principle of state responsibility cannot apply in cyberspace because it has not achieved international consensus regarding its application. Additionally, China places more emphasis on addressing cyber terrorism in a new legally binding instrument than Russia. Overall, both China and Russia strongly push for the progressive development of international law in the form of a new legally binding treaty for cyberspace.

This background paper traces the evolution of Russia and China's perspectives on international law's applicability in cyberspace since the first OEWG in 2019 by reviewing primary sources (including government statements, documents, and OEWG substantive session videos) and secondary sources. Two challenges related to this review should be noted before proceeding. Firstly, China has published far fewer statements and documents on the OEWG's website than Russia. States are not required to publish their statements online, and this process ultimately relies on their own initiative. Therefore, in addition to the available statements, this paper involved analysis of both China and Russia's oral contributions found in OEWG session videos. Secondly, some Chinese and Russian statements required translation into English via online translation tools. Considering linguistic nuances in one language do not always have an equivalent in another language, these translations may contain slight deviations from the original meanings. The background paper proceeds in three sections. Section one analyses Russia's position on international law in cyberspace. Section two identifies China's position on international law in cyberspace and outlines similarities and differences between the Russian and Chinese positions. Section three summarises the main research findings.

1. Background

1.1. The original proposal and first GGE

Before discussing how Russia and China perceive gaps in existing international law, it is important to outline previous discussions on ICTs within the United Nations General Assembly (UNGA). In 1998, Russia proposed a UNGA resolution inviting member states to submit their views on "developing international principles that would enhance the security of global information and telecommunications systems and help combat information terrorism and criminality."[2] Six years later, the UNGA created the first GGE (2004-2005) to study the legal implications of ICT threats. To date, there have been six GGEs and two OEWGs tasked with discussing how ICT developments affect international peace and security.

[2] UNGA 'Developments in the field of information and telecommunications in the context of international security' (4 January 1999) UN Doc A/RES/53/70, p. 2.

Although the first GGE did not produce a consensus report, three subsequent GGEs (2009-2010; 2012-2013; 2014-2015) reached agreement. These groups have addressed current and future cyber threats, how international law applies in cyberspace, confidence and capacity building measures, and norms of responsible State behaviour.[3] This background paper addresses the second sub-topic on how international law applies in cyberspace.

1.2. The second, third, and fourth GGEs

The second GGE (2009-2010) recognised "differences in national laws and practices may create challenges to achieving a secure and resilient digital environment,"[4] but did not mention international law. The third GGE's (2012-2013) consensus report marked a significant milestone by concluding international law and the UN Charter applied in cyberspace.[5] Building on this strong foundation, the fourth GGE (2014-2015) acknowledged the existence of "established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction."[6] This acknowledgement was important because it alluded to IHL's potential application in cyberspace. The consensus report also explained "States must observe principles of international law including state sovereignty, sovereign equality, the settlement of disputes by peaceful means, non-intervention in internal affairs…[and] comply with obligations under international law to respect and protect human rights."[7] Overall, the fourth GGE report went one step further than previous reports by listing international legal principles applicable in cyberspace.

1.3. The fifth GGE, sixth GGE, and two OEWGs

Although the fifth GGE (2016-2017) achieved no consensus report, the sixth GGE (2019-2021) produced a report reaffirming international law's applicability in cyberspace. This report listed principles of international law (including sovereignty, non-interference, peaceful dispute settlement, etc.) applicable in cyberspace.[8] Additionally, this report acknowledged the importance of studying how IHL applied in cyberspace and underscored that "recalling these principles by no means legitimates or encourages conflict."[9] This statement is significant because Russia and China frequently oppose discussing IHL within

[3] UN Office of Disarmament Affairs 'Developments in the field of information and telecommunications in the context of international security' < https://disarmament.unoda.org/ict-security/> accessed 20 March 2024.
[4] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 July 2010) UN Doc A/65/201 para 11.
[5] UNGA 'Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security' (n 1) p. 2.
[6] UNGA 'Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174 para 28.
[7] Ibid.
[8] UNGA 'Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135, p. 17-18.
[9] Ibid para 71.

the OEWG, asserting that such discourse legitimizes armed conflict in cyberspace.[10] In 2018, Russia proposed establishing an OEWG (2019-2021) to continue discussing developments in the field of information and telecommunications in the context of international security which includes international law's applicability in cyberspace. Both the sixth GGE (sponsored by the U.S.[11]) and the first OEWG ran parallel to each other. In March 2024, the second OEWG's (2021-2025) seventh substantive session (chaired by Mr. Burhan Gafoor) took place at UN Headquarters.

[10] Ministry of Foreign Affairs, 'China's Position on International Rules-making in Cyberspace,' The People's Republic of China (November 2021) < https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html> accessed 30 March 2024, section III.

[11] UNGA 'Advancing Responsible State behavior in cyberspace in the context of international security' (22 December 2018) UN Doc A/RES/73/266

2. Russia's approach to international law in cyberspace

Main takeaways

- Russia opposes addressing gender issues and the gender digital divide within the OEWG.
- Russia recently acknowledged that the impact of human rights in cyberspace could be addressed within the OEWG.
- Russia argues that gaps in existing international law relate to attribution, qualifying computer attacks as armed attacks, the responsibility of manufacturers, countering the use of ICTs for terrorist activities, and curtailing the spread of illegal online content.
- Russia argues that the specific and technical nature of the ICT environment requires a new legally binding instrument.
- Russia argues that in the absence of a specific legally binding instrument in the ICT sphere, it is the UN norms of responsible state behavior that form the basis of relevant regulation.
- Russia recognizes that the following international legal principles apply in cyberspace: sovereignty, non-interference in internal affairs, the peaceful settlement of disputes, and the inadmissibility of unsubstantiated accusations against states for wrongful acts with ICTs.
- Russia considers the right to self-defence inapplicable in cyberspace.
- Russia calls for responsible state behavior more generally without explicitly mentioning the phrase 'state responsibility.'
- Both China and Russia advocate for a new legally binding instrument under several OEWG sub-topics (namely discussions on international law, capacity building, and rules, norms, and principles).

2.1. What topics does Russia consider outside the OEWG's mandate?

Before discussing how Russia defines gaps in international law, it is worth mentioning what topics Russia considers outside the OEWG's mandate. For example, Russia opposes addressing gender issues and the gender digital divide.[12] Russian delegates explained that a

[12] The Russian Federation, 'Zero Draft of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (19 January 2021) <

single mention of female representatives participating in OEWG sessions in the report's preamble could be retained as a compromise.[13] Additionally, Russia previously argued that sustainable development and human rights were "secondary to the OEWG."[14] For example, Russia crossed out a reference to ICTs threatening "economic development, livelihoods, and ultimately the safety and well-being of individuals."[15] Regarding human rights, Russia recently published a document stating that discussions on a new legally binding instrument should focus on how to prevent ICTs from harming fundamental human rights like the right to respect for private life.[16] In a joint declaration with the African Union, Russia also declared "cooperation in the field of international information security shall comply with the principles of ensuring human rights and freedoms."[17] This acknowledgement of human rights in cyberspace represents a shift in Russian policy compared to previous documents. For reference, Russia previously argued that human rights "were not directly related to the competence of the UNGA First Committee"[18] and OEWG.

2.2. Where does Russia see gaps in existing international law?

To support the argument that existing international law contains gaps, Russia highlights the following considerations. Firstly, the progressive development of technologies renders the automatic application of existing international law "completely groundless."[19] Secondly, Russia argues that the principle of cooperation in the use of ICTs, "how computer attacks are qualified from the point of view of international law," and "how State activities in

---

https://front.un-arm.org/wp-content/uploads/2021/02/RF-OEWG-zero-draft-report-with-the-Russian-amendments-ENG.pdf> accessed 30 March 2024, para 11.

[13] The Russian Federation, 'First Meeting of the Fifth Substantive Session' (24 July 2023) <http://webtv.un.org/en/asset/k1o/k1ovl7bhl9> accessed 30 March 2024.

[14] The Russian Federation, 'Commentary of the Russian Federation on the Zero Draft of the Open-Ended working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,' (8 February 2021) < https://front.un-arm.org/wp-content/uploads/2021/02/Russian-commentary-on-the-OEWG-zero-draft-report-ENG.pdf> accessed 30 March 2024, para 7.

[15] The Russian Federation (n 13) para 22.

[16] The Russian Federation, 'Updated Concept of the Convention of the United Nations on Ensuring International Information Security' (7 March 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian_Federation.pdf> accessed 30 March 2024, section II para 7.

[17] The Russian Federation and African Union, 'Declaration of the Second Russia-Africa Summit on Cooperation in the Field of International Information Security," (28 July 2023) < http://en.kremlin.ru/supplement/5975> accessed 2 April 2024, para 1.

[18] The Russian Federation, 'Concept of work of the UN Open-ended Working Group on security of and in the use of information and communication technologies 2021-2025,' (1 June 2021) < https://documents.unoda.org/wp-content/uploads/2021/06/Concept-paper-on-the-New-OEWG-ENG.pdf> accessed 15 April 2024, p. 5.

[19] The Russian Federation, 'Statement by the Delegation of the Russian Federation at the sixth session of the UN open-ended working group on security of and in the use of ICTs,' (13 December 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-__statement_-_IL_-_ENG.pdf> p. 3.

the use of ICTs are considered unlawful from the point of view of international law" remain unknown.[20] Thirdly, Russia argues that there is currently no "trustworthy and unequivocal identification" process for attributing malicious cyber activity, reinforcing the importance of establishing internationally agreed norms.[21] Other gaps mentioned by Russia include "the responsibility of manufacturers for the reliability and safety of their products, the lack of universally recognized norms for countering the use of ICTs for terrorist attacks, [and] the dissemination of illegal content and fakes."[22] Overall, Russia pushes for the "progressive development of international law" in the form of a new legally binding instrument for cyberspace.[23]

Russia routinely crosses out sentences in draft reports that mention conducting in-depth discussions between States to further develop a common understanding of how international law applies in cyberspace.[24] Additionally, Russia crosses out references to States developing their own understanding of how international law applies in cyberspace and "contributing to building consensus within the international community."[25] Without a legally binding instrument, Russia argues that the UN norms of responsible State behaviour provide the only basis for consideration and relevant regulation.[26] Thus, Russia opposes highlighting the non-binding nature of such norms because this undermines their importance and invites States to follow them less stringently.[27] On this point, Russia argues that Western states advocate exclusively for the voluntary nature of these norms and "want to take the role of arbitrators."[28] When developing this new legally binding instrument, Russia considers it inappropriate for the International Law Commission to clarify how

[20] The Russian Federation, 'Statement on Applicability of International Law' (7 December 2022) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf> accessed 30 March 2024, p. 2.
[21] The Russian Federation, 'Statement by the representative of the Russian Federation at the informal intersessional meeting of the Open-ended working group on security of and in the use of ICTs 2021-2025' (7 December 2022) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf > p. 1-2.
[22] The Russian Federation (n 22) p. 2.
[23] The Russian Federation, 'Intervention on Introduction of Draft APR2,' (24 July 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-_statement_-_introduction_24.07.2023_-_ENG.pdf> accessed 30 March 2024, p. 3.
[24] The Russian Federation (n 13) para 35.
[25] Ibid, para 40.
[26] The Russian Federation (n 15) para 4.
[27] Ibid.
[28] The Russian Federation (n 14).

international law applies in cyberspace because these discussions should be reserved only for States.[29]

Currently, Russia opposes the full applicability of existing international law in cyberspace due to the "legal and technical specifics of the information environment."[30] Although Russia agrees "existing universally recognized norms and principles of international law fixed in the UN Charter"[31] apply in cyberspace, this seems to only extend to sovereignty, non-interference in internal affairs, the peaceful settlement of disputes, and the inadmissibility of unsubstantiated accusations against states for wrongful acts with ICTs. It is important to note that Russia's interpretation of sovereignty differs from the Western approach. Russia considers state sovereignty paramount and absolute,[32] meaning less binding international mechanisms and interference equates to more state sovereignty.[33] This approach mirrors the Westphalian approach to sovereignty whereby States possess a monopoly of force within their borders. Conversely, the contemporary Western approach prioritises protecting individuals and limiting the exercise of sovereign power through checks and balances.[34] These different interpretations of sovereignty illustrate how countries endorse sovereignty in cyberspace while holding unique understandings on its practical implementation.

2.3. Self-defence and International Humanitarian Law

Russia considers the right to self-defence inapplicable in cyberspace because existing methods of attributing malicious activity are not reliable or timely. Additionally, Russia notes that existing international law does not explain when using ICTs would amount to an armed attack under Article 51 of the UN Charter.[35] Therefore, Russia argues that "the use of the right

[29] The Russian Federation, 'Commentary of the Russian Federation on the Initial 'Pre-Draft' of the Final Report of the UN OEWG,' (2020) < https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf> accessed 30 March 2024, p. 3.
[30] The Russian Federation, 'Statement on Applicability of International Law,' (13 December 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-__statement_-_IL_-_ENG.pdf> accessed 30 March 2024, p. 2.
[31] The Russian Federation, 'Statement by the Representative of the Russian Federation at the online discussion of the second 'pre-draft' of the final report of the UN Open-ended working group on developments in the field of information and telecommunications in context of international security,' (15 June 2020) < https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf> accessed 30 March 2024, p. 3.
[32] Lauri Mälksoo, *Russian Approaches to International Law* (OUP 2015), p. 101; Mikael Baaz, 'International Law is Different in Different Places: Russian Interpretations and Outlooks' (2016) International Journal of Constitutional Law 262, 269.
[33] Ibid, p. 100.
[34] Ibid, p. 19.
[35] The Russian Federation, 'Statement on Applicability of International Law,' (7 March 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Russian_statement_How_international_law_applies.pdf> accessed 30 March 2024, p. 3.

for self-defence in response to information attacks may lead to armed escalation"[36] and cannot be endorsed.

In addition to self-defence, Russia opposes discussing IHL's application in cyberspace because there are "no grounds" for such discussions.[37] More specifically, Russia argues that, as IHL only applies in armed conflicts, discussing IHL legitimises cyberwarfare and military applications of ICTs.[38] As for due diligence obligations, Russia argues that there is uncertainty on "what States should do when information infrastructure within their territory is used to carry out computer attacks belonging to a foreign company."[39] To jumpstart negotiations on a new legally binding instrument for international law in cyberspace, Russia has proposed developing universal terminology in UN consensus reports.

2.4. State responsibility

Russia calls for responsible state behaviour more generally (i.e., by referencing the UN norms of responsible State behaviour) but does not explicitly mention the principle of state responsibility. For example, Russia argues that "States should reaffirm the rights and responsibilities of all States, in accordance with the universally recognized norms and rules."[40] Additionally, Russia argues that "all States must play an equal role in, and carry equal responsibility for, international governance of the Internet."[41] In another statement, Russia criticised the Zero Draft Report of the OEWG and argued that the phrase "shared responsibilities between States" needed clarification or should be removed.[42] Russia also crossed out a reference in the OEWG draft report to changing or elaborating on the rules of responsible State behaviour in the future.[43] At the sixth session of the OEWG in December 2023, Russia came close to explicitly mentioning state responsibility by announcing "it is unacceptable to assign responsibility for incidents in information space to anyone without evidence."[44] Overall, Russia implies state responsibility cannot be applicable in cyberspace

[36] The Russian Federation, 'Compilation of Views on All Agenda Items,' (14 December 2021) < https://documents.unoda.org/wp-content/uploads/2021/12/Russia-statements-OEWG-13-17.12.2021-Eng.pdf> accessed 30 March 2024, p. 12.
[37] The Russian Federation, 'Fourth Meeting of the Fourth Substantive Session' (7 March 2023) <https://webtv.un.org/en/asset/k1k/k1k81rqtz0> accessed 30 March 2024.
[38] Ibid.
[39] The Russian Federation (n 32) p. 2.
[40] The Russian Federation, 'Contribution of the Russian Federation on rules, norms and principles of responsible behavior f states in the information space,' (1 January 2021) < https://documents.unoda.org/wp-content/uploads/2022/03/Russian-contribution-on-rules-of-behaviour-Eng.pdf> accessed 2 April 2024, para 5.
[41] Ibid, para 6.
[42] The Russian Federation (n 13) para 10.
[43] The Russian Federation, 'Draft report of the OEWG on developments in the field of information and telecommunications in the context of international security,' (9 February 2021) <https://front.un-arm.org/wp-content/uploads/2021/02/RF-Revised-consensus-aimed-OEWG-draft-report-ENG.pdf> accessed 8 April 2024, para 46.
[44] The Russian Federation (n 21) p. 3.

by highlighting attribution difficulties and the lack of a legally binding instrument for cyberspace.

2.5. Russia's advocacy efforts under several OEWG sub-topics

Finally, Russia pushes for new legally binding instrument under several OEWG sub-topics including discussions on international law and rules, norms, and principles. This decision is significant because it underscores Russia's stance that any substance on norms must be linked to making a new legally binding instrument. For example, in one statement on rules, norms, and principles Russia argued for "the development of a universal international legal act regulating activities of states in the ICT-sphere." [45] In another statement, Russia noted that "it is obvious that the existing voluntary and non-binding rules of behaviour are not enough…the solution to this problem [is to develop] an international legal regime for regulating information space."[46] Russia has also reiterated the "unjustified bias in favour of implementing only the existing list of voluntary, non-binding rules of behaviour"[47] rather than focusing on making the norms legally binding.[48] Overall, Russia seizes every opportunity to advocate for a new legally binding instrument in OEWG discussions.

[45] The Russian Federation, 'Statement by the head of the Russian interagency delegation to the first substantive session of the UN OEWG,' (20 March 2022) <https://documents.unoda.org/wp-content/uploads/2022/03/Russia-OEWG-statement-3-30.03.2022-Eng.pdf> accessed 9 April 2024, p. 3.
[46] The Russian Federation, 'Statement by the representative of the Russian Federation at the Fourth Session of the United Nations Open-ended working group 2021-2025,' (7 March 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Russian_statement_Rules_norms_and_principles.pdf > accessed 9 April 2024, p. 2.
[47] The Russian Federation, 'Statement by the delegation of the Russian Federation at the sixth session of the UN Open-ended working group on security of and in the use of ICTs 2021-2025,' (12 December 2023), < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-__statement_-_norms_-_ENG.pdf> accessed 9 April 2024, p. 2.
[48] The Russian Federation, 'Statement by the Russian Delegation at the seventh session of the United Nations Open-ended working group 2021-2025,' (5 March 2024) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-__statement_-_norms_05.08.2024_-_ENG.pdf> accessed 9 April 2024, p. 2.

3. China's approach to international law in cyberspace

Main takeaways

- China employs a more cautious rhetoric than Russia.
- China opposes discussing sustainable development, gender equality, and human rights within the OEWG.
- China argues that emphasising the voluntary nature of norms of responsible State behaviour sends an unconstructive message that a new legally binding instrument is unachievable.
- As for gaps in existing international law, China points to accountability difficulties in cyberspace, the lack of an agreed-upon definition for illegal network behaviour, and the inability to address cyber terrorism by curtailing the spread of illegal online content.
- In agreement with Russia, China affirms that the existing international law on sovereignty, non-interference in internal affairs, the peaceful settlement of disputes, and the inadmissibility of unsubstantiated accusations against States for wrongful acts with ICTs all applies in cyberspace.
- China argues that state responsibility has not gained international consensus and cannot be applied in cyberspace.
- China is actively pushing for cyber terrorism to be addressed in a legally binding instrument.
- China argues that the applicability of IHL and *jus ad bellum* needs to be handled with prudence without escalating or legitimating cyber conflicts.
- Both China and Russia advocate for a new legally binding instrument under several OEWG discussion topics (namely those on international law, capacity building, and rules, norms, and principles).

3.1. What topics does China consider outside the OEWG's mandate?

Before discussing how China defines gaps in international law, it is worth mentioning what topics China considers outside the OEWG's mandate. China opposes discussing sustainable development, human rights, and gender equality in the OEWG.[49] Taking a less assertive stance than Russia, China argues that "in the long run, these issues are important…however, these are anything but the priority of this group."[50] Additionally, China

[49] The People's Republic of China, 'China's Contributions to the Initial Pre-Draft of the OEWG,' (2021) < https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf> accessed 30 March 2024, p. 1.
[50] Ibid, p. 1.

argues that there are "other mechanisms under the UN framework"[51] working on these issues and that therefore these do not need to be addressed within the OEWG.

3.2. Where does China see gaps in existing international law?

China's argument for a new legally binding treaty is two-fold. Firstly, China criticises other countries for emphasising the voluntary nature of the norms of responsible State behaviour, arguing that it sends an "unconstructive message"[52] that a new legally binding instrument is unachievable. Secondly, China argues that maintaining international peace and security requires considering the unique attributes of cyberspace.[53] These attributes include accountability difficulties and disagreement on defining illegal network behaviours and cyber-attacks.[54] Therefore, China argues that relevant, existing international laws and new legally binding norms should be applied simultaneously.[55] As for relevant international law, China affirms that sovereignty, the peaceful settlement of disputes, no threat or use of force, non-intervention in the internal affairs of other states, the inadmissibility of unsubstantiated accusations against States for wrongful acts with ICTs, and peaceful dispute settlement apply in cyberspace.[56] China defines sovereignty in cyberspace as States exercising jurisdiction over ICT infrastructure and activities within their territories, passing ICT-related public policies, and protecting critical ICT infrastructure against interference and damage.[57] As for state responsibility, China argues that this concept has not gained international consensus and cannot be applied in cyberspace.[58] Additionally, China holds that there is no international agreement defining illegal cyber behaviours.[59] Given this lack of international agreement, China reaffirms the eleven UN norms of responsible state behaviour must be fully followed.[60]

---

[51] Ibid, p. 1.
[52] Ibid, p. 3.
[53] The People's Republic of China, 'Fifth Meeting of the Fourth Substantive Session,' (8 March 2023) < https://webtv.un.org/en/asset/k19/k191pqmwp8> accessed 30 March 2024.
[54] The People's Republic of China,'中国代表团在联合国信息安全开放式工作组首次会议关于国际法适用的发言,' (16 December 2021) < https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-7th-plenary-meeting_international-law_DEC-16-AM_CHN.pdf> accessed 30 March 2024, p. 2.
[55] The People's Republic of China (n 51) p. 4.
[56] The People's Republic of China, 'China's Submissions to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,' (2021) < https://front.un-arm.org/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf> accessed 31 March 2024, p. 6.
[57] Ibid, p. 3.
[58] The People's Republic of China (n 51) p. 5.
[59] The People's Republic of China (n 56) p. 2.
[60] The People's Republic of China, '中国代表团在联合国信息安全问题 开放式工作组二期会上的发言,' (28 March 2022) < https://documents.unoda.org/wp-content/uploads/2022/04/Chinas-statement_ICT-OEWG_2nd-Substantive-Session.pdf> accessed 9 April 2024, p. 2.

3.3. Cyber terrorism

China prioritises addressing cyber terrorism in a new legally binding instrument more than Russia. This stronger emphasis is evident in Russia's endorsement of China's contribution to the International Code of Conduct (A/69/723) which explained "States should cooperate in combating criminal and terrorist activities with the use of ICTs."[61] In 2017, China published an international strategy detailing cooperation in cyberspace, arguing that "efforts should be made to prevent terrorists from using the Internet to spread extremist ideology, or plan and orchestrate cyber terrorist activities."[62] This document supported increasing policy exchanges and law enforcement cooperation between States to combat cyber terrorist activities.[63] When reiterating the importance of addressing cyber terrorism in a new legally binding instrument,[64] China argues that "States should request Internet service providers to cut off the online dissemination channel of terrorist content by closing propaganda websites and deleting terrorist and violent extremist content."[65]

3.4. International Humanitarian Law

Another point of commonality between China and Russia relates to the inapplicability of IHL in cyberspace. Whereas Russia has adopted a more assertive stance on IHL's inapplicability, China pursues a more tentative approach. In 2021, China explained "States should handle the applicability of the law of armed conflicts and jus ad bellum with prudence and prevent escalation or turning cyberspace into a new battlefield."[66] In 2023, China stated that "we must be cautious about applying the law of armed conflict" in cyberspace because this provides "a veneer of legitimacy for a certain country"[67] to engage in cyber conflicts. While Russia refers to "Westerners"[68] in similar accusations, China criticises other countries more vaguely.

---

[61] The Russian Federation (n 42) para 3.
[62] Ministry of Foreign Affairs of the People's Republic of China, 'International Strategy of Cooperation on Cyberspace,' (1 March 2017) < https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html> accessed 28 March 2024, chapter IV section 5.
[63] Ibid.
[64] The People's Republic of China, 'China's Positions on International Rules-Making in Cyberspace,' (20 October 2021) <https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html> accessed 26 March 2024.
[65] UNGA 'Chair's Summary: Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (8-12 March 2021)' (10 March 2021) < https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf> accessed 30 March, p. 16.
[66] The People's Republic of China (n 58) p. 6.
[67] The People's Republic of China (n 55)
[68] See The Russian Federation, 'Statement by Dr. Vladamir Shin, Deputy Director, Department of International Information Security, Ministry of Foreign Affairs of the Russian Federation at the online-consultation of the Open-ended working group on development in the field of information and telecommunications in the context of international security,' (19 February 2021) < https://front.un-arm.org/wp-

3.4. China's advocacy efforts under several OEWG sub-topics

Similarly to Russia, China pushes for a new legally binding instrument under several OEWG sub-topics including discussions on international law, rules, norms and principles, and confidence-building measures. In a statement on rules, norms, and principles China explained that "the Working Group should focus on transforming past consensus into politically binding norms."[69] Additionally, in a statement on confidence-building measures (CBM) China argued that "CBM should not replace the formulation of international rules for cyberspace…the two can complement each other."[70] This illustrates China and Russia's push for a new legally binding instrument in all facets of the OEWG.

Conclusion

Both Russia and China support creating a new legally binding instrument on international law in cyberspace due to alleged "gaps" in existing international law. According to their statements, these gaps include tracing malicious activity, defining illegal cyber behaviour, establishing a threshold for an armed attack in cyberspace under the UN Charter, curtailing the spread of illegal online content, establishing the responsibility of manufacturers, countering the use of ICTs for terrorist activities, and addressing the specific and unique attributes of the technology environment.

content/uploads/2021/02/Russian-Federation-statement-at-informal-OEWG-session-19.02.2021.pdf> acceded 9 April 2024, p. 3.

[69] The People's Republic of China, '中国代表团在联合国信息安全开放式工作组 首次会议关于负责任国家行为规范的发言,' (15 December 2021) <https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-5th-plenary-meeting_rules-norms-and-principles-of-responsible-behavior-of-states_DEC-15-AM_CHN.pdf> accessed 9 April 2024, p. 1.

[70] The People's Republic of China, '中国代表团在联合国信息安全开放式工作组首次会议关于建立信任措施的发言,'(16 December 2021) < https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-8th-plenary-meeting_confidence-building-measures_DEC-16-PM_CHN.pdf > accessed 9 April 2024, p. 1.

List of primary sources

United Nations

UNGA 'Developments in the field of information and telecommunications in the context of international security' (4 January 1999) UN Doc A/RES/53/70

UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 July 2010) UN Doc A/65/201

UNGA 'Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98

UNGA 'Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174

UNGA 'Advancing Responsible State behavior in cyberspace in the context of international security' (22 December 2018) UN Doc A/RES/73/266

UNGA 'Chair's Summary: Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (8-12 March 2021)' (10 March 2021) < https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf> accessed 30 March 2024

UNGA 'Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135

UN Office of Disarmament Affairs 'Developments in the field of information and telecommunications in the context of international security' < https://disarmament.unoda.org/ict-security/> accessed 20 March 2024

United States of America

The United States, 'Statement on Applicability of International Law,' (30 March 2022) < https://documents.unoda.org/wp-content/uploads/2022/04/US-remarks-for-March-OEWG-intl-law.pdf> accessed 30 March 2024

European Union

The European Union, 'Statement on Applicability of International Law by European Union,' (23 May 2023) <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/23_05_24_OEWG_ICTs_Cyber_Intersessional_EU_statement_International_Law_SG_DHoD_-_FINAL.pdf> accessed 30 March 2024

Russian Federation

The Russian Federation, 'Commentary of the Russian Federation on the Initial 'Pre-Draft' of the Final Report of the UN OEWG,' (2020) < https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf> accessed 30 March 2024

The Russian Federation, 'Statement by the Representative of the Russian Federation at the online discussion of the second 'pre-draft' of the final report of the UN Open-ended working group on developments in the field of information and telecommunications in context of international security,' (15 June 2020) < https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf> accessed 30 March 2024

The Russian Federation, 'Contribution of the Russian Federation on rules, norms and principles of responsible behavior f states in the information space,' (1 January 2021) < https://documents.unoda.org/wp-content/uploads/2022/03/Russian-contribution-on-rules-of-behaviour-Eng.pdf> accessed 2 April 2024

The Russian Federation, 'Zero Draft of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (19 January 2021) < https://front.un-arm.org/wp-content/uploads/2021/02/RF-OEWG-zero-draft-report-with-the-Russian-amendments-ENG.pdf> accessed 30 March 2024

The Russian Federation, 'Commentary of the Russian Federation on the Zero Draft of the Open-Ended working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,' (8 February 2021) < https://front.un-arm.org/wp-content/uploads/2021/02/Russian-commentary-on-the-OEWG-zero-draft-report-ENG.pdf> accessed 30 March 2024

The Russian Federation, 'Draft report of the OEWG on developments in the field of information and telecommunications in the context of international security,' (9 February 2021) <https://front.un-arm.org/wp-content/uploads/2021/02/RF-Revised-consensus-aimed-OEWG-draft-report-ENG.pdf> accessed 8 April 2024

The Russian Federation, 'Statement by Dr. Vladamir Shin, Deputy Director, Department of International Information Security, Ministry of Foreign Affairs of the Russian Federation at the online-consultation of the Open-ended working group on development in the field of information and telecommunications in the context of international security,' (19 February 2021) < https://front.un-arm.org/wp-content/uploads/2021/02/Russian-Federation-statement-at-informal-OEWG-session-19.02.2021.pdf> acceded 9 April 2024

The Russian Federation, 'Concept of work of the UN Open-ended Working Group on security of and in the use of information and communication technologies 2021-2025,' (1 June 2021) < https://documents.unoda.org/wp-content/uploads/2021/06/Concept-paper-on-the-New-OEWG-ENG.pdf> accessed 15 April 2024

The Russian Federation, 'Compilation of Views on All Agenda Items,' (14 December 2021) < https://documents.unoda.org/wp-content/uploads/2021/12/Russia-statements-OEWG-13-17.12.2021-Eng.pdf> accessed 30 March 2024

The Russian Federation, 'Statement on Applicability of International Law' (7 December 2022) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf> accessed 30 March 2024

The Russian Federation, 'Statement on Applicability of International Law,' (13 December 2022) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-_statement_-_IL_-_ENG.pdf> accessed 30 March 2024

The Russian Federation, 'Statement on Applicability of International Law,' (7 March 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Russian_statement_How_international_law_applies.pdf> accessed 30 March 2024

The Russian Federation, 'Updated Concept of the Convention of the United Nations on Ensuring International Information Security' (7 March 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf> accessed 30 March 2024

The Russian Federation, 'Fourth Meeting of the Fourth Substantive Session,' (7 March 2023) <https://webtv.un.org/en/asset/k1k/k1k81rqtz0> accessed 30 March 2024

The Russian Federation, 'Statement by the representative of the Russian Federation at the Fourth Session of the United Nations Open-ended working group 2021-2025,' (7 March 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Russian_statement_Rules_norms_and_principles.pdf > accessed 9 April 2024

The Russian Federation, 'Statement by the head of the Russian interagency delegation to the first substantive session of the UN OEWG,' (20 March 2022) <https://documents.unoda.org/wp-content/uploads/2022/03/Russia-OEWG-statement-3-30.03.2022-Eng.pdf> accessed 9 April 2024

The Russian Federation, 'Updated Concept of the Convention of the United Nations on Ensuring International Information Security: Proposal of the Russian Federation with Co-Sponsors' (29 June 2023) <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf> accessed 30 March 2024

The Russian Federation, 'First Meeting of the Fifth Substantive Session' (24 July 2023) <http://webtv.un.org/en/asset/k1o/k1ovl7bhl9> accessed 30 March 2024

The Russian Federation, 'Intervention on Introduction of Draft APR2,' (24 July 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-_statement_-_introduction_24.07.2023_-_ENG.pdf> accessed 30 March 2024

The Russian Federation and African Union, 'Declaration of the Second Russia-Africa Summit on Cooperation in the Field of International Information Security," (28 July 2023) < http://en.kremlin.ru/supplement/5975> accessed 2 April 2024

The Russian Federation, 'Statement by the delegation of the Russian Federation at the sixth session of the UN Open-ended working group on security of and in the use of ICTs 2021-2025,' (12 December 2023), < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-___statement_-_norms_-_ENG.pdf> accessed 9 April 2024

The Russian Federation, 'Statement on Applicability of International Law,' (13 December 2023) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-___statement_-_IL_-_ENG.pdf> accessed 30 March 2024

The Russian Federation, 'Statement by the Russian Delegation at the seventh session of the United Nations Open-ended working group 2021-2025,' (5 March 2024) < https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-___statement_-_norms_05.08.2024_-_ENG.pdf> accessed 9 April 2024

People's Republic of China

Ministry of Foreign Affairs of the People's Republic of China, 'International Strategy of Cooperation on Cyberspace,' (1 March 2017) < https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html> accessed 28 March 2024

Ministry of Foreign Affairs, 'China's Position on International Rules-making in Cyberspace,' The People's Republic of China (November 2021) < https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html> accessed 30 March 2024

The People's Republic of China, 'China's Submissions to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,' (2021) < https://front.un-arm.org/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf> accessed 31 March 2024

The People's Republic of China, 'China's Contributions to the Initial Pre-Draft of the OEWG,' (2021) < https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf> accessed 30 March 2024

The People's Republic of China, 'China's Positions on International Rules-Making in Cyberspace,' (20 October 2021) <https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html> accessed 26 March 2024

The People's Republic of China, '中国代表团在联合国信息安全开放式工作组 首次会议关于负责任国家行为规范的发言,' (15 December 2021) <https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-5th-plenary-meeting_rules-norms-and-principles-of-responsible-behavior-of-states_DEC-15-AM_CHN.pdf> accessed 9 April 2024

The People's Republic of China, '中国代表团在联合国信息安全开放式工作组首次会议关于建立信任措施的发言,'(16 December 2021) < https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-8th-plenary-meeting_confidence-building-measures_DEC-16-PM_CHN.pdf > accessed 9 April 2024

The People's Republic of China,'中国代表团在联合国信息安全开放式工作组首次会议关于国际法适用的发言,' (16 December 2021) < https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-7th-plenary-meeting_international-law_DEC-16-AM_CHN.pdf> accessed 30 March 2024

The People's Republic of China, '中国代表团在联合国信息安全问题 开放式工作组二期会上的发言,' (28 March 2022) < https://documents.unoda.org/wp-content/uploads/2022/04/Chinas-statement_ICT-OEWG_2nd-Substantive-Session.pdf> accessed 28 March 2024

The People's Republic of China, 'Fifth Meeting of the Fourth Substantive Session,' (8 March 2023) < https://webtv.un.org/en/asset/k19/k191pqmwp8> accessed 30 March 2024

Bibliography

Baaz M, 'International Law Is Different in Different Places: Russian Interpretations and Outlooks' (2016) 14 International Journal of Constitutional Law 262.

Mälksoo L, *Russian Approaches to International Law* (OUP 2015).

University of Glasgow

LEUPHANA
UNIVERSITÄT LÜNEBURG

INSTITUT
BARCELONA
ESTUDIS
INTERNACIONALS

ULB UNIVERSITÉ
LIBRE
DE BRUXELLES

UNIVERSITY
OF TARTU
1632

Radboud Universiteit

Co-funded by
the European Union