This publication was funded in 2025 by the Russia Strategic Initiative, U.S. European Command. The views expressed in this publication do not necessarily represent the views of the Department of War or the United States Government.

From Normative to Operational: The Sino-Russian "No-Limits" Partnership in Cyberspace and its Limitations

David Song-Pehamberger
Deputy Director, Community of Interest for Strategy & Defense
European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

March 2026

Since the beginning of Russia's full-scale invasion of Ukraine, Beijing and Moscow have arguably grown closer to each other than they have been since the end of the Cold War. China has become Russia's lifeline, supplying it with everything from dual-use goods to consumer electronics, while Russia has become a significant source of hydrocarbons and an increasingly important and reliable export market for Chinese industries. Both states' leaders have repeatedly emphasized their "*no limits*" partnership.[1] Xi Jinping and Vladimir Putin further agreed to enhance cooperation in "*strategic sectors*," including cyberspace.[2] Already back in 2015, they publicly pledged to cooperate on global internet governance and to refrain from attacking each other in cyberspace.[3] The reality of their cooperation in this domain, however, is more complicated than their no-limits partnership would suggest.

The virtually limitless partnership: Reshaping internet governance together

The strategic partnership between Beijing and Moscow in the international legal domain predates the war in Ukraine. Although China and Russia have somewhat differing grand strategic objectives regarding the global world order they envision, they have worked hand-in-hand toward their goals in many instances. China is a revisionist power seeking to incrementally change global governance in its favor, while Russia is aggressively attacking the current system to undo the Western-led order, in the hope to emerge as the major power it seeks to be. Both are united in their opposition to Western-led, democratic, and human rights-centric multilateralism, and have mostly supported each other's actions in the UN, especially since Xi Jinping came to power.[4]

Beijing has consistently reaffirmed the UN's role as the only legitimate forum for multilateralism, as well as the centrality of the UN Charter to international law. Therefore, China's ambitions to change global governance were not about discarding the Charter or even changing its content, but to alter states' interpretation of it. While Western democracies continue to view the UN Charter as the foundation of universal values and human rights, China emphasizes national sovereignty, non-interference, and *true multilateralism*. Beijing wants these principles to be recognized as absolute and unquestionable. This means that governments have the right to exercise absolute sovereignty over their territory, and that no other state or group of states may, under any circumstances, interfere with their internal affairs. This also entails rejecting the Security Council's authority, under Chapter VII of the UN Charter, to intervene in a state's internal affairs in the event of a threat to international peace, or indeed for any other reason, such as human rights violations. Beyond interference in national affairs, exclusive groupings such as the Security Council or other committees or working groups, which are not open to all countries, should be seen as illegitimate and rejected in favor of the UN General Assembly (UNGA), which includes all 193 member states of the UN.

These goals have been repeatedly reaffirmed under the 'Shared Future for Mankind' framework, first presented by Xi in 2013.[5] This blueprint for China's preferred form of global governance contains the foundational pillars of Governance, Civilization, Security, and Development, which have been expanded into China's big 'Global Initiatives' over the past years.[6] And during the 2015 World Internet Conference, Xi introduced China's vision to

"*jointly build a community of shared future in cyberspace*," as the extension of this framework to cyberspace.[7]

Unlike the generally accepted understanding by Western democracies of cyberspace being a shared common good, usually with added emphasis on human rights, China's framework highlights absolute state sovereignty over national cyberspace and seeks to reject any influence of non-governmental bodies. As such, Beijing has over the years, among others, attempted to move internet governance and standards-setting from non-governmental and multi-stakeholder organizations, such the IETF and ICANN,[8] to the UN's state-led International Telecommunication Union (ITU), and push for authoritarian-leaning standards in cyberspace.[9] This also relates to China's push for a *safe*, *clean,* and *civilized* internet. Crucially, the arbiter of what constitutes *safe* or *civilized* conduct, in Beijing's view, is always the government of the national cyberspace in question.[10]

Another example is China's Global Data Security Initiative (GDSI), which centers on, again, absolute sovereignty of governments over all digital data within states' territories, as opposed to the usual Western focus on the right to privacy.[11]

Russia's agenda within the UN appears to have been less focused on such a specific blueprint, but its diplomats have largely supported China's drafts and statements aimed at approaching its 'Shared Future' framework within the UN. In addition, Moscow has consistently pushed for legitimizing authoritarian approaches to global governance, including in cyberspace, and successfully contributed to chipping away at exclusive groups' legitimacy within the UN. One relevant example is the case of the cyber working groups.

The UN Group of Governmental Experts (GGE) on security related to Information and Communication Technologies (ICT) was established in 2004 and was active in six iterations of two-year durations each.[12] Just as with other thematic GGEs in the UN, it contained only a selected few states with specific interest or expertise in the given subject matter, and it also frequently consulted with non-governmental experts. The resolutions that the GGE developed were presented to the UNGA and were therefore considered and voted on by all UN states. Nonetheless, Russia and China have questioned the GGE's legitimacy, due to its exclusive nature, and pushed for working groups to be open to all governments, with the emphasis being on governments (i.e. excluding multi-stakeholders and non-governmental entities). Among the ICT GGE's successes were the 11 norms of responsible state behavior in cyberspace, as well as the conclusion that international law fully applies to cyberspace, both of which were presented in the form of resolutions that were unanimously adopted by all states of the UNGA in 2015 and 2021, respectively.[13]

Then in 2019, based on Russia's initiative, the ICT Open-Ended Working Group (OEWG) was launched. Unlike the GGE, it was open to all UN states throughout all sessions. The first OEWG ran concurrently with the final GGE until 2021, after which the OEWG was renewed for a new four-year term, while the GGE ceased to exist. Russia had successfully opened the discussion up to all UN states. China, Russia, and several Western states sponsored delegates of developing countries to join the working group sessions in New York.[14] While the OEWG was much more inclusive than the GGE in this regard, it was government-led, with a minor

role for non-governmental institutions, which were given minimal speaking time, and their participation had to be approved by all states. Russia made repeated use of this *de facto* veto power. During OEWG sessions, the understanding of international law and best practices in cyberspace arguably backslid, as Russia, China, and other likeminded authoritarian states repeatedly questioned the legitimacy of the GGE's past resolutions, based on its exclusionary nature – ignoring the fact that the GGE's resolutions were adopted by consensus by all states, including those now doubting their validity. A repeated demand by Russia and China during the OEWG was the establishment of a new, legally binding treaty on international law in cyberspace. Western countries consistently pushed back, as this would question and dilute the universal applicability of international law. China also kept pushing its contents contained in the Shared Future framework and the GDSI. Beijing and Moscow were also successful in reducing undesired language, such as human rights, international humanitarian law, and any references to universal values, which was reduced with each annual working group report. The OEWG concluded in 2025, with its final report establishing the permanent 'UN Global Mechanism on Cybersecurity,' which will hold its first session in March 2026. China and Russia succeeded, among others, in including a mandate to discuss the need for new, legally-binding norms in cyberspace.[15]

In between, Russia was also successful in its demand for negotiating a Cybercrime Convention, also known as the 'Hanoi Convention,' which was concluded in 2024.[16] While this treaty ultimately did not achieve Moscow's more authoritarian demands, it did succeed in questioning existing norms on cybercrime, including related to the Budapest Convention on Cybercrime, and potentially set a precedent that Russia and China now keep referring to in their ongoing demands to negotiate a binding treaty on international law in cyberspace.

While the example of China-Russian cyber cooperation in the international legal domain showcases their alignment to shape cyberspace in the authoritarian image, their cooperation was far from integrated. Both sides have repeatedly introduced their own agendas and blueprints for future mechanisms and treaties, demonstrating that there was no clear leader in this alliance, nor was there comprehensive alignment. However, within the working groups, as is the case in the UNGA in general, the two never criticized each other publicly, and they usually settled on a mutual authoritarian compromise to their lines by the end of the week of each week-long OEWG session, which they then pushed against the Western-led bloc.

However, while in terms of global cyber governance China and Russia may appear partners on somewhat equal footing, in actual cyberspace Beijing has long pulled ahead.

The fortification and weaponization of China's cyberspace

The CCP's efforts to strengthen its control over the domestic cyberspace and expand capabilities for global power projection went hand-in-glove. The push for global dominance in cyberspace started in earnest, as elsewhere, following the ascent of Xi Jinping.

Within a year of coming to power, Xi ordered a rapid tightening of the CCP's control over China's cyberspace. In August 2013, Xi remarked that "*the internet has become the main battlefield for the public opinion struggle*." Within the same month, the government issued

strict new regulations that closed off what freedoms had remained in Chinese social media. And in 2015, the government cracked down on the VPNs that many citizens had used to circumvent the so-called Great Firewall of China.[17]

Since then, the CCP introduced a series of laws that cemented its grip over all aspects of domestic cyberspace. The 2015 National Security Law expanded the authority of the state's security apparatus, and the 2017 National Intelligence Law obliged all citizens, companies, and organizations to fully cooperate with intelligence authorities whenever requested. China's Cybersecurity Law, also passed in 2017, further stipulated that all data created in and related to China would have to be stored within China, and that security services must be given full access to data when demanded. This essentially marked the end of end-to-end encryption and digital anonymization in China. The state's control over China's cyberspace was sealed in 2021, when the Personal Information Protection Law and the Data Security Law were enacted. They codified the requirements to store all personal and "*important*" data locally and to play a role in "*protecting the state*."[18] And in 2023, the Counterespionage Law was updated to ban the export of any data related to national security.[19] These legislative acts deliberately remained vague on what constitutes important or national security-relevant data, thereby further strengthening the state's authority to arbitrarily control the nation's cyberspace.

At the same time, the Chinese government has pushed hard to remove the country's dependence on American hardware and software suppliers and to create technology supply chains free from Western input. For critical sectors, including energy and finance, state-owned firms have even been ordered to remove foreign software, including operating systems, from their systems.[20]

And while the CCP has worked hard to remove foreign dependencies, it also systematically utilized national legislation to weaponize software vulnerabilities. In 2021, national authorities responsible for China's cyberspace, public security, and information technology published a national vulnerability disclosure regulation. Similar to other countries' vulnerability disclosure requirements, it stipulates that vulnerabilities discovered by private firms or individuals must be shared with authorities – in China's case within 48 hours. Later amendments further reduced the required reporting time to one hour for vulnerabilities related to critical infrastructure.[21]

However, unlike global best practices, access to China's vulnerability database is broadly shared with national security authorities known to engage in offensive cyber activities, including the Ministry of State Security (MSS) and the People's Liberation Army (PLA). In addition, the MSS actively funds vulnerability research and requires its many private cyber security partner firms to regularly provide it with software vulnerabilities. This approach appears to yield thousands of vulnerabilities annually, some of which have shown to have been weaponized in the past. And over recent years, private cyber security firms and researchers have been increasingly restricted from sharing discovered vulnerabilities with partners outside of China.[22] China has, in effect, amassed a treasure trove of software vulnerabilities, the true scale of which is unknown.

At the same time, China's capabilities for reaching into foreign networks were greatly enhanced. The PLA's cyber forces were expanded and placed under direct authority of China's supreme military command, under Xi's chairmanship.[23] Meanwhile, civilian offensive

capabilities were significantly expanded, as part of China's Military-Civil Fusion Strategy. This included the MSS, once a rather obscure spy agency tasked with keeping taps on dissidents, which under Xi became a world-leading cyber spying powerhouse.[24] It also involved a myriad of private firms, which have increasingly been used as proxies for both cyber[25] and information[26] operations against foreign targets. This kind of civilian diffusion broadened China's offensive cyber capabilities, while also complicating Western efforts at attributing and countering Chinese attacks.

Within a decade, China grew from a *de facto* cyber middle power to arguably the most sophisticated and capable cyber threat actor, who continuously exploits the complex grayzones of cyberspace. Through the fortification of China's cyberspace, and the amassing of both capabilities and tools, Chinese cyber actors were successfully deployed in foreign systems around the world.

Most notably, China weaponized vulnerabilities to conduct some of the widest-ranging espionage campaigns ever executed, including the single most significant case of cyber espionage known to date, Salt Typhoon. In this yearslong attack, hackers linked to the MSS stole personal data of nearly every American citizen, alongside data of government and private networks of over 80 other countries.[27] In addition, cyber security authorities of the US and its Five Eyes partners have uncovered the Chinese threat actor Volt Typhoon, which had pre-positioned itself in multiple critical infrastructure systems across the US, with the potential to disrupt telecommunication, transportation, energy, and water supplies.[28] Many more countries have recently attributed serious cyber attacks against their critical national networks to China, including the UK, Canada, Australia, Germany, Czechia, the Netherlands, Japan, and South Korea, to name only a few examples from just the past year.[29]

However, China's reach into foreign networks is not limited to its ideological adversaries. Its no-limits partner Russia was likewise repeatedly targeted by China's cyber spies, although Moscow has never publicly attributed such attacks to Beijing.

The Limitations of No-Limits

It is a well-known fact that since the beginning of Russia's full-scale invasion of Ukraine, in February 2022, both Russian and Chinese cyber attacks against Western democracies have sharply increased. But so have Chinese cyber attacks against Russian government agencies and private companies. Much of these hostile activities appear to be aimed at stealing Russian technology and insights into the war in Ukraine. Known incidents of Chinese state-affiliated cyber operations against Russia include attempts at stealing sensitive information related to nuclear submarines, satellite communication, electronic warfare, aviation, and other fields related to the defense sector.[30]

Behind closed doors, Moscow is well aware of its no-limits partner's malign activities. A leaked FSB planning document from 2023-2024 has warned of the serious threat posed by China, which is even referred to as "*the enemy*." It noted Chinese attempts at recruiting Russian spies and take advantage of disaffected scientists to obtain military secrets and sensitive

technologies.[31] The FSB has, in turn, focused on uncovering potential Chinese spies, including through harvesting WeChat data.[32]

Notwithstanding the aforementioned public pledge by Beijing and Moscow to steer clear from each other's cyberspace, China keeps attacking Russia. It is unclear whether Russia is repaying its strategic partner in kind, but Russian cyber operations are unlikely to pose a similar danger to China. Russia's offensive operations are focused on Ukraine and its Western partners, and China's national cyberspace hides behind a fortified Great Firewall, supported by formidable digital firepower, the rapid development of which likely surprised Moscow as much as it did the West. Only a decade ago, Washington's national intelligence assessment was that Russia would continue to be a far more dangerous cyber threat than China.[33] However, within just a few years, this assessment has been flipped on its head, as China has become the most advanced global cyber threat actor.[34]

Furthermore, since 2022, Beijing's and Moscow's approaches to offensive Cyber operations have significantly diverted. China remains a risk-averse and clandestine cyber threat actor, covering its tracks and wanting to be seen as a responsible great cyber nation, at least by most states. Russia, on the other hand, has become aggressive and disruptive, prioritizing sabotage operations and exploiting whatever vulnerabilities it gains access to.[35] Given these opposite approaches, it appears unlikely that China would consider cooperating closely with Russia on operational cyber activities. China possesses world-leading offensive cyber capabilities and has stockpiled a massive stash of exploitable vulnerabilities. Its cyber actors likely have breached many more sensitive networks around the world than is currently known. It is, therefore, difficult to imagine how Moscow could be trusted with such powerful cyber weapons, especially if it continues to struggle winning ground in Ukraine and opposing European sanctions. However, in case of an open conflict between China and, say, the US, Russia may indeed become a valuable ally that could quickly adopt Chinese cyber tools and amplify China's own offensive cyber capabilities.

For the time being, cooperation in the normative domain will likely continue, as it remains mutually beneficial and has already paid off in the form of ongoing authoritarian creep in the international arena. But closer integration in operational or technological areas is currently of little benefit to Beijing and may even come with significant risks to its long-term strategic ambitions. On top of that, behind the façade of authoritarian solidarity, both sides have ample reason to mistrust each other, whether in cyberspace or beyond.

It is unclear what the Russian leadership thinks of its ambiguous relationship with China, or how it discreetly communicates its dissatisfaction to Beijing. However, based on the situation Putin finds himself in, he likely has little choice either way. Putin's Russia still seeks to be seen as a major global power; it wants to dismantle the Western-led international order, which remains a threat to its expansionist ambitions; and it needs to secure regime survival in the face of Western sanctions. For all these, Russia needs China's help. It is an unequal relationship. Even if China continues to attack Russia in the shadows and exploit its current vulnerabilities to steal what little technological advantage it still possesses, Moscow cannot fight back publicly. These are the limitations of Russia's no-limits partnership with China.

[1] Antoni Slodkowski and Laurie Chen, "China's Xi affirms 'no limits' partnership with Putin in call on Ukraine war anniversary," *Reuters* (24 February 2025): https://www.reuters.com/world/xi-putin-hold-phone-call-ukraine-war-anniversary-state-media-says-2025-02-24/

[2] Matthew Johnson, "PRC and Russia Operationalize Strategic Partnership," *Jamestown* (14 May 2025): https://jamestown.org/prc-and-russia-operationalize-strategic-partnership/

[3] Olga Razumovskaya, "Russia and China Pledge Not to Hack Each Other," *The Wall Street Journal* (8 May 2015): https://www.wsj.com/articles/BL-DGB-41673

[4] Evgeny Roshchin, "The Implications for Global Governance of China and Russia's Post-2022 Alignment," *CEPA* (23 June 2025): https://cepa.org/comprehensive-reports/the-implications-for-global-governance-of-china-and-russias-post-2022-alignment/

[5] Liza Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies," *Texas National Security Review* (November 2018): https://tnsr.org/2018/11/xis-vision-for-transforming-global-governance-a-strategic-challenge-for-washington-and-its-allies/

[6] The Global Development Initiative (2021), Global Security Initiative (2022), Global Civilization Initiative (2023), and Global Governance Initiative (2025) are all based on the pillars of the framework of the 'Community of Common Destiny for Mankind' (now officially referred to as 'Shared Future' in English).

[7] Dakota Cary, "Community watch: China's vision for the future of the internet," *Atlantic Council* (4 December 2023): https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/

[8] The multi-stakeholder Internet Engineering Task Force (IETF) is the premier internet protocol standards-setting organization, while the Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization managing the internet's Domain Name System (DNS).

[9] Kai von Carnap, Antonia Hmaidi, Rebecca Arcesati, and Jeroen Groenewegen-Lau, "Fragmenting cyberspace," *MERICS* (30 November 2023), 40-42: https://merics.org/sites/default/files/2023-12/MERICS%20Report_Future%20of%20the%20internet_final%20%281%29.pdf

[10] "Community watch," *Atlantic Council* (2023).

[11] Arjun Kharpal, "China accuses U.S. of 'bullying' as it touts new global data security push," *CNBC* (7 September 2020): https://www.cnbc.com/2020/09/08/china-launches-global-data-security-initiative-to-counter-us-pressure.html

[12] Their full proper names are the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' and the 'Open-ended working group on security of and in the use of information and communications technologies,' respectively.

[13] "UN global mechanism on cybersecurity," *Digital Watch* (accessed on 12 February 2026): https://dig.watch/processes/un-gge

[14] "UNIDIR delivers training to Women in Cyber Fellows in New York," *UNIDIR* (15 August 2025): https://unidir.org/unidir-delivers-training-to-women-in-cyber-fellows-in-new-york/

[15] This summary of the OEWG is based on the author's observations at the OEWG sessions during 2023-2025. All related documents, papers, presentations, and working group reports can be found here: "Open-Ended Working Group on Information and Communication Technologies: Documents," *UNODA* (accessed on 14 February 2026): https://meetings.unoda.org/meeting/57871/documents

[16] Gatra Priyandita and Bart Hogeveen, "The UN cybercrime convention: a victory for state sovereignty," *The Strategist* (16 August 2024): https://www.aspistrategist.org.au/the-un-cybercrime-convention-a-victory-for-state-sovereignty/

[17] Elizabeth C. Economy, "The great firewall of China: Xi Jinping's internet shutdown," *The Guardian* (29 June 2018): https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

[18] "Fragmenting cyberspace," *MERICS* (2023), 15-17.

[19] Laurie Chen, "China approves wide-ranging expansion of counter-espionage law," *Reuters* (27 April 2023): https://www.reuters.com/world/asia-pacific/china-passes-revised-counter-espionage-law-state-media-2023-04-26/

[20] Liza Lin, "China Intensifies Push to 'Delete America' From Its Technology," *The Wall Street Journal* (7 March 2024): https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f

[21] William Zheng, "China's internet watchdog mandates 1-hour reporting for serious cybersecurity incidents," *SCMP* (15 September 2025): https://www.scmp.com/news/china/politics/article/3325596/chinas-internet-watchdog-mandates-1-hour-reporting-serious-cybersecurity-incidents

[22] Dakota Cary and Kristin Del Rosso, "Sleight of hand: How China weaponizes software vulnerabilities," *Atlantic Council* (6 September 2023): https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/

[23] J. Michael Dahm, "A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force," *Jamestown* (26 April 2024): https://jamestown.org/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/

[24] Chris Buckley and Adam Goldman, "How China's Secretive Spy Agency Became a Cyber Powerhouse," *The New York Times* (28 September 2025): https://www.nytimes.com/2025/09/28/world/asia/how-chinas-secretive-spy-agency-became-a-cyber-powerhouse.html

[25] Matt Brazil and Peter W. Singer, "China is turning to private firms for offensive cyber operations," *Defense One* (30 June 2024): https://www.defenseone.com/threats/2024/06/china-turning-private-firms-offensive-cyber-operations/397767/

[26] Gaute Friis, Nickson Quak, Sara Shah, and Elliot Stewart, "Countering China's Use of Private Firms in Covert Information Operations," *Stanford* (21 June 2024): https://stacks.stanford.edu/file/druid:fg865kf5598/countering_prc_use_of_private_firms%20in_IO_gordian_knot_center_ver.pdf

[27] Adam Goldman, "'Unrestrained' Chinese Cyberattackers May Have Stolen Data From Almost Every American," *The New York Times* (4 September 2025): https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html

[28] "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," *CISA* (7 February 2024): https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[29] For a more comprehensive overview, see: "Significant Cyber Incidents," *CSIS* (accessed on 8 February 2026): https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[30] Megha Rajagopalan, "China Unleashes Hackers Against Its Friend Russia, Seeking War Secrets," *The New York Times* (19 June 2025): https://www.nytimes.com/2025/06/19/world/europe/china-hackers-russia-war-ukraine.html

[31] Jacob Judah, Paul Sonne, and Anton Troianovski, "Secret Russian Intelligence Document Shows Deep Suspicion of China," *The New York Times* (7 June 2025): https://www.nytimes.com/2025/06/07/world/europe/china-russia-spies-documents-putin-war.html

[32] Aaron Krolik and Paul Sonne, "Russian Intelligence Says It Collects WeChat Data. What Does That Mean?" *The New York Times* (7 June 2025): https://www.nytimes.com/2025/06/07/world/europe/russia-china-wechat-spying.html

[33] Siobhan Gorman, "Intel Chief: Russia Tops China as Cyber Threat," *The Wall Street Journal* (17 October 2024): https://www.wsj.com/articles/BL-WB-49926

[34] Michael Martina, Patricia Zengerle, and Erin Banco, "China poses biggest military, cyber threat to US, intel chiefs say," *Reuters* (26 March 2025): https://www.reuters.com/world/china-presents-top-military-cyber-threat-united-states-us-report-says-2025-03-25/

[35] Seth G. Jones, "Russia's Shadow War Against the West," *CSIS* (18 March 2025): https://www.csis.org/analysis/russias-shadow-war-against-west