LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Universiteit Leiden

Russian Perspectives on China as an Actor in Cyberspace

Eric Siyi Zhang | Dr. Rogier Creemers

January 2021

Summary

Although the so-called 'Sino-Russian approach' to internet governance is often simplistically understood as a "black-box coalition" seeking to upend the multi-stakeholder and rule-based order, the realities of the Sino-Russian interactions in cyberspace are much more complicated. On one hand, their common distrust towards the liberal world order and the US hegemony forms the basis for cooperation at the multilateral level, especially on norm-promotion of cyber-sovereignty and a state-based internet governance model. Recently, China and Russia have also intensified their cooperation on regulating online content. On the other hand, from the Russian perspective, there are also several factors, for example perceived cyberespionage and China's geo-economic prowess, that undermine bilateral trust or hinder further Sino-Russian cooperation. Based on Russian-language academic and policy literature, this report unpacks the multifaceted Sino-Russian relation in cyberspace from a Russian perspective, and provides recommendations for more effective engagement with both countries.

Introduction

In global cyber affairs, Russia and China are often seen as the nexus of an alliance that seeks to upend the multi-stakeholder, rules-based order on which the Internet has been based. As they are both opposed to the substance of liberal norms as well as the predominance of the United States in the digital sphere, they have joined together to work towards a new form of ordering, based on a strict reading of national sovereignty and a greater role for national governments. Particularly in multilateral forums such as the UN, both countries have often operated together, proposing draft codes of conduct for state behaviour in cyberspace in 2011 and 2015, and voting for the establishment of an Open-Ended Working Group on cyber affairs in 2018, in contrast to the already existing Group of Governmental Experts (GGE).

However, earlier reports [1] have suggested substantial differences exist between both countries on matters of practical policy. China, for instance is rapidly becoming a global digital economy and technology leader, while Russia's digital sector is small. This has significant consequences for their role as global actors. Furthermore, while both countries share a common ideological heritage rooted in Soviet-style Marxism, there are significant cultural differences between both. A more granular understanding of the relationship between Moscow and Beijing would therefore be useful to more accurately assess both countries' positions, and different possibilities for engagement.

This report intends to contribute to such an understanding by surveying Russian perspectives on China as a cyber actor. Drawing on Russian language source material, it reviews first the common basis China and Russia share in both ideological and geopolitical terms. Subsequently, it analyses how Russia perceives China both in the bilateral context, and as a partner in the multilateral environment. It concludes by offering recommendations for policy makers to more effectively take into account Sino-Russian dynamics in global cyber policy making.

Geopolitical and Ideological Basis of Sino-Russian Cyber Cooperation

As cyberspace has steadily played a more significant role in states' efforts

[1] Broeders, D., L. Adamson, R. Creemers. 2019. Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace. The Hague Program for Cyber Norms Policy Brief. November 2019.

in ensuring national security, economic prosperity, and social stability, cybersecurity, or information security – the preferred term of Russia and China - has become a topic of high political prominence. On several key geopolitical questions, there is a considerable degree of proximity between both countries' position, as well as a shared ideological and historical background that leads them to share a broadly common understanding of the problem they face.

The most important point of agreement between China and Russia in geopolitics is their distrust towards US hegemony in the physical world and cyberspace, which has provided an adequate basis for them to cooperate on a number of issues. Furthermore, global political developments in recent years reinforced the sense of a common adversary: according to the Russian International Affairs Council (RIAC), many Russian experts and scholars observe that the Ukrainian Crisis in 2014 has made Russia pivot its geopolitical focus to the East and drawn the Sino-Russian relation closer.[2] A similar point could be made about the US pivot to Asia. In the realm of technology, ongoing Sino-American decoupling will also have lasting negative implications for China's relation with the West, and push China not only towards greater indigenization, but also to interact more closely with Russia. The upcoming Biden presidency might shave off some of the harder edges of recent US policy but will not fundamentally change the increasingly adversarial take on China in Washington, which is a rare point of bipartisan consensus.

Outside of hard interests and imperatives, there is also a strong family resemblance between both countries' ideological outlook and worldview on cyber affairs, which draws back to the close relationship between the nascent People's Republic and the USSR in the 1950s. As such, the terminological similarities in the policy languages of Moscow and Beijing are not only shared choices of vocabularies, but also reflect common understandings in issues of interests, objects, or values to be secured, and threats to be tackled. Both China and Russia adopt a wider definition of cybersecurity than the mostly technical one known in the West, i.e., the correct functioning of the internet and the infrastructure. For China and Russia, apart from the security of network systems, data and infrastructure, information on the Internet itself also matters. In other words, they attach non-technical, information-based elements to their definition of cybersecurity. [3] In Russian official documents, such as the doctrine of information security, and bilateral and

[2] RIAC & Fudan University. (2014). 中俄关系研究报告 [Research report on Sino-Russian relations].

[3] Bulavin, A. V. (2014). О подходах США и Китая к обеспечению кибербезопасности [On approaches of The USA and China to cybersecurity]. Obshchestvo: Politika, ekonomika, parvo: 2014. № 1, pp. 27-31.

multi-lateral agreements that Russia has entered into with China, or in statements by members of the Shanghai Cooperation Organisation (SCO), the equivalent to the English word cybersecurity in the Russian language, kiberbezopasnost' [кибербезопасность], is never used, and all references to the concept of cybersecurity adopt the term information security [информационная безопасность], instead.[4] China, for its part, has nearly exclusively used the term "cybersecurity" [网络安全] in official policy usage in 2014[5], but habitually used "information security" before then[6]. Its national cybersecurity strategy equally defines security threats first and foremost in function of the harm to economic, social, and political processes, rather than in technical terms.

There are thus both ideological and geopolitical drivers for the Sino-Russian cooperation in cyberspace. The 2015 Sino-Russian cyber treaty reflects a set of common official views, and has defined 'information security' as follows:

> 'Information Security - describes the practice of defending the information of individuals, society and the government from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.'[7]

[4] President of Russia. (2016). Указ Президента Российской Федерации от 05.12.2016 г. № 646 Об утверждении Доктрины информационной безопасности Российской Федерации [Presidential Decree of Russian Federation from 05 Dec. 2016 No. 646 about adopting the Doctrine of Information security of the Russian Federation]. Retrieved from: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf

[5] A new top-level coordinating body for digital affairs, established in 2014, was called the Cybersecurity and Informatization Leading Group. China's national strategy for security in cyberspace also adopts this term. Cyberspace Administration of China. (2016). Guojia wangluo kongjian anquan zhanlüe [National Cyberspace Security Strategy]. Retrieved from: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

[6] See, for instance, State Council (2012). Guanyu dali tuijin xinxihua fazhan he queshi baozhang xinxi anquan de ruogan yijian [Some Opinions concerning Forcefully Moving Informatization Development Forward and Realistically Guaranteeing Information Security]. Retrieved from: https://chinacopyrightandmedia.wordpress.com/2012/06/28/some-opinions-concerning-forcefully-moving-informatization-development-forward-and-realistically-guaranteeing-information-security/.

[7] Government of Russia. (2015). On signing the Agreement between the Government of the Russian

China and Russia's inclusion of information as a part of cybersecurity can be motivated by the perceived threat of foreign interference in internal affairs, as explicitly mentioned in the 2015 Sino-Russian cyber treaty; the treaty expressed concerns about the use of information technology to 'undermine the sovereignty and security of states and interference in their internal affairs and infringement of the privacy of citizens, destabilize the political and socio-economic situation, inciting ethnic and religious hatred'.[8]

Deepening cooperation on online content, Russia and China signed a further treaty in 2019.[9] Unlike the 2015 treaty, the full text of the 2019 treaty is unavailable through open sources. However, press releases indicate the use of Chinese technology to facilitate Russian online content regulation is at least one main area of cooperation.

Furthermore, the Chinese cyber-administration and the Russian Ministry of digital development, communication and mass media signed the *Wuxi joint declaration* [Усийская совместная декларация/无锡共识] in November 2019. The joint declaration called for more cooperation between Chinese and Russian online media, and the deepening of mutual knowledge of each other among ordinary Chinese and Russian people. It also called for more coordination between Chinese and Russian mass media in reporting regional and international events in order to enhance the rhetorical power [языковое право/话语权] of China and Russia's online media.[10] Already in 2017, the Chinese Media Group [中央广播电视总台] and Russia Today created an online media platform – Sinorusfocus [Россия-Китай: главное/中俄头条].[11] In 2019, the Chinese Media Group and Rossiyskaya Gazeta created a joint news studio in Moscow, Zhong'e Ruiping [中俄锐评/Россия-Китай: события и комментарии]. Both publish commentaries and news articles on issues of mutual importance on different Chinese and Russian

---

Federation and the Government of the People's Republic of China on cooperation in ensuring international information security. Retrieved from: https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf

[8] Ibid.

[9] RIA Novosti. (2019). В Роскомнадзоре оценили опыт Китая в сфере регулирования интернета [Chinese experience in the sphere of regulating the internet is valued at Rozkomnadzor]. Retrieved from: https://ria.ru/20191021/1560012016.html.

[10] Wuxi Joint Declaration. (2019). Retrieved from: https://d-russia.ru/wp-content/uploads/2019/11/usiyskaia_declaratciia.pdf.

[11] Sinorusfocus. (n.d.). Россия-Китай: главное [Russia-China: top stories]. Retrieved from: https://www.sinorusfocus.com/index.html.

online and traditional media platforms.[12]

However, these commonalities should not obscure the fact that there are also significant geopolitical and ideological differences between both sides. In some cases, this is due to the different nature of their global role: Russia is primarily a military power with a comparatively insignificant economy, while China is rapidly achieving a more comprehensive great power status. While China considers itself as a rising global power that will eventually attain equal status with the US in a bi-polar world order, Russia has been seeing the world order as a multi-polar one in the making since the end of the Cold War[13]. This perception is at least partly self-flattering, as it retains a rule for Russia as a major power on the world stage.

Contrary to the common misperception that Russia and China are a 'united front' against the Western liberal order, the two countries are far from allies. From the Russian perspective, many anxieties and uncertainties remain ahead in the Sino-Russian relationship. First, many Russia experts are still wary of China's great power status, and uncertain about how Russia should live with this new reality. Russia's state-sponsored thinktank, the RIAC, wrote the report *Theses of Russian Foreign Policy (2012 - 2018), that* points out that a Sino-Russian alliance or a close partnership is undesirable for Russia, as the growing asymmetry of power in China's favour would eventually make Russia the junior partner that depends on China politically and economically.[14] Besides, Russia also keeps a close watch on China's rising sentiment of nationalism and the possible change it will bring to China's foreign policy. Some Russian scholars believe that China's swift growth of nationalism/patriotism under the slogan of the 'great rejuvenation of the Chinese nation' is dangerous to the parts of the world surrounding China and brings an end to Deng's diplomacy of *taoguang yanghui* (keeping a low profile).[15]

Moreover, much as this idea is scorned in Europe, Russia ultimately sees itself

[12] Xinhua. (2019). 中央广播电视总台与俄罗斯报社“中俄锐评”联合评论工作室正式揭牌亮相 [The joint commentary studio of Chinese Media Group and Rossiyskaya Gazeta Zhong'e Ruiping is launched]. Retrieved from: http://www.xinhuanet.com/2019-06/06/c_1124593717.htm

[13] Broeders et al. (2019).

[14] Russian International Affairs Council. (2012). Тезисы о внешней политике России (2012 – 2018 гг.) [Theses on foreign policies of Russia (2012 – 2018)], p.21.

[15] Portyakov, V. Ya. (2013). Становление Китая как ответственной глобальной державы [China becoming a responsible global power]. Institute of Far East, Russian Academy of Science, p.118.

as a culturally, historically, and spiritually European country. There are areas, for example a custom, or even economic union, in which building a high-level alliance with China is not on Russia's agenda[16]. Also, the escalation of Russian-Western tension after 2008 seemed to have pushed Russia's foreign policy to shift to Eurasianism [Евразийство][17], which seeks to enhance the level of integration with post-Soviet states.[18] However, it does not seem that this includes enhancement of Russia's strategic-level connectivity with China or other partners in Asia. For example, despite Russia's more amicable political relation with China, it has not echoed China's consistent call for economic integration either bilaterally or under the framework of the SCO, whereas an economic community from Lisbon to Vladivostok was on the Russian agenda during the 2000s.[19] In Central Asia, Russia has also been wary of the growing economic influence of the BRI in what Russia perceives as its own sphere of influence. In short, whereas the common distrust towards US hegemony in cyberspace incentivises China and Russia to cooperate in highly politicised areas such as cybersecurity and international law, and despite the ostensibly close relationship between Xi Jinping and Vladimir Putin, Russia and China fundamentally lack the political proximity and economic connectivity to form a broad-spectrum alliance, or to develop a comprehensive positive agenda for global governance, be it in economic or digital affairs, climate change and other pressing areas.

From Partner to Cyber Criminal – Russian Perspectives on China in Cyberspace

Before elaborating on discussions in Russia about China's role in the cyberspace, it must be mentioned that, perhaps surprisingly[20], academic and think tank writers have devoted surprisingly little attention to this topic. The amount of literature that discusses China's role in the cyberspace stands

[16] Schubert, J., & Savkin, D. (2016). Dubious economic partnership: Why a China-Russia free trade agreement is hard to reach. *China Quarterly of International Strategic Studies*, 2(04), 529-547.
[17] Eurasianism is understood as the reintegration of Russia with post-Soviet states, it does not include the rest of Asia which was never a part of the USSR, such as China and Japan.
[18] Kaczmarski, M. (2017). Non-western visions of regionalism: China's New Silk Road and Russia's Eurasian Economic Union, International Affairs 93: 6, pp.1357–1376.
[19] RIAC & Fudan University. (2014). 中俄关系研究报告 [Research report on Sino-Russian relations]. p.44.
[20] The same thing is, however, true in reverse: very few Chinese writers have devoted attention to the Russian role in global cyber affairs.

in stark contrast to the much greater quantity of writings discussing the role of the US. Similarly, there is very little engagement between Chinese and Russian researchers on cyber policy, in comparison with the relatively numerous track 1.5 and track 2 processes taking place with the US and European countries. One can only speculate as to the reasons why: it may well be that this is seen as a sensitive topic. Certainly, at the popular level, ordinary Chinese and Russian citizens are distant from and lack knowledge of, or interest in each other. Another important reason can be the lack of Russian scholars who can speak Chinese and understand the technicality of cybersecurity at the same time. Furthermore, Russian scholars who study Sino-Russian relations are traditionally more preoccupied with geopolitics and economic cooperation, and cybersecurity is still an underdeveloped topic.[21] For the most part, the extant literature on this topic originates from thinktanks, especially the Russian International Affairs Council (RIAC).

Unsurprisingly, these writings mostly echo the mainstream positions in both Moscow and Beijing. For instance, according to the 2017 report of *Sino-Russian Dialogue* - a joint project of the RIAC and Fudan University, the deepening of the Sino-Russian cooperation in cybersecurity is motivated by consensus on the threats in the area of cybersecurity. Such consensus is expressed in the following aspects: (1) the rejection of the hegemonial role of the US in the global cyberspace, (2) the multilateral governance of the internet, (3) the objection to using cyber technologies to interfere with other states' internal affairs, and (4) the support for the norm of cyber-sovereignty. However, there are also several obstacles for Russia to build higher level of trust towards China in cyberspace, such as perceived Chinese cyberespionage and concerns around the digital economy.

The Norm of Cyber Sovereignty

China and Russia both have, at least rhetorically, adopted a classical Westphalian reading of two elements of sovereignty in cyberspace: the supreme authority of national governments within their own territories, and the sovereign equality of states at the international level. This conflicts with the Western profession of universal values and rights in cyberspace, including freedom of speech and access to information. This distinction does not just apply in cyberspace but reflects readings of human rights between both sides in general.

With the coordination and support of other countries of the SCO, China and Russia have sought to establish sovereignty as a foundational norm in cyber governance, submitting two Codes of Conduct to the UNGA which advocated the recognition of states' sover-

[21] Ye. A. Razumov, personal communication, Dec 4, 2020.

eign right in the policy authority of internet-related public issues.[22] The urgency for sovereignty has increased throughout the 2010s, often catalysed by political events elsewhere in the world. An example of this was the significant role of information technology in political movements such as the Arab Spring and Ukraine's revolution, which Russia and China see as Western projects to subvert governments that do submit to Western hegemony. To them, this highlights what undesired online information might be able to cause in their own territories. Cyber-sovereignty is often discussed in Russia and China in the context of tackling foreign interference in what they see as internal affairs, in which cyber-sovereignty provides important normative and rhetoric basis.

On the other hand, one should refrain from assuming that the Sino-Russian likeminded-ness in the **norm** of cyber-sovereignty implies that they agree or need to agree on the **how** that cyber sovereignty is realized at home. On the contrary, cyber-sovereignty entails that states have no say in how each other regulate their own cyberspace. Currently, there is no consensus on whether the 'Chinese model' – characterised simplistically by Russian experts, particularly on the liberal side of the political spectrum, as prohibiting citizens' access to foreign digital services and information, is desirable for Russia, as adopting the 'Chinese model' seriously undermines Russia's already-limited internet freedom, and will be economically costly.[23] Apart from the debated desirability, there are also questions about the feasibility of doing so: Russia does not have domestic alternatives to provide to its citizens if the government bans foreign social media platforms and search engines, such as Facebook and Google.[24]

Although this narrative is largely absent in official sources, as mentioned above, among many frequently cited scholarly publications and popular independent media outlets, China's political regime in general, and China's policies in cyberspace are depicted as totalitarian. However, in contrast to Western commentators, Russian writers, on the off chance they do engage in this narrative, rarely assert that the perceived Chinese digital totalitarianism is a looming threat or urge China

[22] United Nations. (2011). Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. Retrieved from: https://www.russemb.org.uk/data/doc/internationalcodeeng.pdf.

[23] Bovt, G. (2019). Китайское чудо. Чему стоит учиться у Поднебесной, а чему нет [Chinese miracle – what is worth learning from the Celestial Empire, and what not]. Retrieved from: https://vm.ru/world/763562-kitajskoe-chudo-chemu-stoit-uchitsya-u-podnebesnoj-a-chemu-net.

[24] Ye. A. Razumov, 04 Dec. 2020, personal communication

to change. Instead, Chinese totalitarianism is usually presented as a mere fact or an assumption. Interestingly, the understanding of China's policies of cybersecurity as totalitarian may simply be borrowed by Russian scholars from American literature, since the bulk of Russian academic publication on China's cybersecurity policies do rely on American literature.

Internet Governance Models

The Sino-Russian like-mindedness not just covers questions on norms, but also on institutional arrangements in cyber governance. Both countries have strongly advocated for a more prominent role of the UN in the global governance of the internet, opposing the multi-stakeholder model supported by the "like-minded states" bloc.

The multi-stakeholder model is currently the de facto governance model of the internet. In the area of the domain name system, it is characterised by the role played by the International Corporation for Assigned Names and Numbers (ICANN) and how ICANN is organised: ICANN coordinates the maintenance and assignment of namespaces and numerical spaces of the Internet, ensuring the functioning of the internet.[25] What makes ICANN a multi-stakeholder organisation is that internet operators are the organisation's only real constituencies, whereas states merely play an advisory role.[26] Maintaining this status quo has become a matter of national policy. In the US National Cyber Strategy, the US expressed its determination to 'ensure that the multi-stakeholder model of Internet governance prevails against attempts to create state-centric frameworks'.[27] However, the internationalisation of ICANN has not diffused Russia's concern that the US is 'able' to cut off Russia's internet. At least, it has had little effect on Russia's policy course to build its sovereign internet – the RuNet[Рунет]: it is not good enough for Russia that the US does not have the keys to Russia's internet, Russia must have them themselves.

Because of their distrust towards the multi-stakeholder model and the US's dominant role therein, Russia and China have promoted reforms and alternatives towards a more multilateral governance system of the internet. The

[25] ICANN. (2019). Bylaws for Internet Corporation for Assigned Names and Numbers. Retrieved from: https://www.icann.org/resources/pages/governance/bylaws-en

[26] Dekker, B.; Okano-Heijmans, M.; Zhang, S. (2020). Unpacking China's Digital Silkroad. Clingendael Report. Retrieved from: https://www.clingendael.org/sites/default/files/2020-07/Report_Digital_Silk_Road_July_2020.pdf

[27] US Government. (2018). National Cyber Strategy of the United States of America, p.25. Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

2011 Shanghai Cooperation Organisation's (SCO) International code of conduct for information security submitted to the UNGA problematised the unequal distribution of internet resources under the multi-stakeholder model and proposed the promotion of a multilateral alternative. It was mentioned that 'states should promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet'.[28]

The debate about multilateral and multi-stakeholder Internet governance was not just a political matter, but also an economic one. Not just authoritarian states such as Russia, China and Iran favour multilateral governance of the internet, other developing countries have equally proposed multilateral reforms, notably Brazil's NetMundial Initiative and India's proposal that the International Telecommunication Union (ITU) should take over the governance of global cyberspace.[29]

Online Content Regulation

The most important element of cyber sovereignty hitherto has been control over online content. During the 6th Wuzhen Internet Conference in 2019, news outlets from Russia and other countries widely covered the treaty between the Cyberspace Administration of China and the Federal Service for Supervision of Communications, Information Technology and Mass Media of Russia (Roskomnadzor) in 'combatting the spread of prohibited information'.[30] However, according to its press secretary Ampelonsky, Roskomnadzor and the Chinese cyberspace administration had already worked together closely over the past few years on this issue,[31] and the treaty merely consolidates this ongoing cooperation.

Exactly what has been included in the treaty has not been made available in

[28] United Nations. (2011). Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. Retrieved from: https://www.russemb.org.uk/data/doc/internationalcodeeng.pdf.

[29] Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. Chin. Polit. Sci. Rev. 1, pp. 88-89.

[30] Authors' translation of соглашение о сотрудничестве в области противодействия распространению запрещенной информации

[31] Deutsche Welle. (2019). Роскомнадзор вместе с Китаем поборется с запрещенной информацией [Rozkomnadzor combats forbidden information together with China]. Retrieved from: www.dw.com/ru/роскомнадзор-вместе-с-китаем-поборется-с-запрещенной-информацией/a-50739440.

open sources. However, as Roskomnadzor head Aleksandr Zharov said that Russia has a lot to learn from China in Internet regulation, especially in terms of technology,[32] it does seem that using Chinese technology to facilitate Russian online content regulation is at least one main area of cooperation. The 2019 treaty[33] also seems like a logical development after the 2015 treaty: Not only did the 2015 treaty affirm national jurisdiction on information, it has also called for technology exchange and cooperation between the "competent authorities" on both sides as a key area of cooperation.[34] Perhaps, Russia was previously unwilling to adopt a Chinese-style firewall in Russia because it was perceived as economically costly and there are significant differences between the political regimes of China and Russia.[35] The Roskomnadzor head said that regulation in Russia is 'softer' and that 'everything that is not prohibited is allowed'.[36] However, it has been widely observed that the Russian internet filtering system introduced in 2012 was largely ineffective. Compared with its Chinese counterpart, Roskomnadzor does not have the powerful infrastructure to block websites in time and has to rely more on legislative rather than technical censorship tools.[37]

---

[32] RIA Novosti. (2019). В Роскомнадзоре оценили опыт Китая в сфере регулирования интернета [Chinese experience in the sphere of regulating the internet is valued at Rozkomnadzor]. Retrieved from: https://ria.ru/20191021/1560012016.html.

[33] In Russian – Соглашение, the English equivalent is agreement. However, as most English-speaking experts refer to the inter-governmental document signed by China and Russia as a treaty, this report also refers to the document signed in 2019 as a treaty.

[34] Government of Russia. (2015). On signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security. Retrieved from: https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf

[35] Bovt, G. (2019). Китайское чудо. Чему стоит учиться у Поднебесной, а чему нет [Chinese miracle – what is worth learning from the Celestial Empire, and what not]. Retrieved from: https://vm.ru/world/763562-kitajskoe-chudo-chemu-stoit-uchitsya-u-podnebesnoj-a-chemu-net

[36] RIA Novosti. (2019). В Роскомнадзоре оценили опыт Китая в сфере регулирования интернета [Chinese experience in the sphere of regulating the internet is valued at Rozkomnadzor]. Retrieved from: https://ria.ru/20191021/1560012016.html.

[37] Birger, P. (2015). Старший товарищ: китайский план цензуры для россий-

In general, it seems that Russia has decided to take a more active approach in regulating online content in recent years. It has introduced tougher Internet laws, requiring search engines to delete some search results, messaging services to share encryption keys,[38] and the controversial bill 'on the right to be forgotten' that allows Russian citizens to press online platforms to remove internet pages that contain 'illegal, inaccurate or irrelevant' personal information.[39] It has also fined Google and blocked Telegram for not co-operating. After the conclusion of the 2019 treaty, while urging people to refrain from speculation about China's role in the Russian internet, Maria Zakharova, spokeswoman of the Russian Ministry of Foreign Affairs, confirmed that there is great potential for cooperation between China and Russia in this area, and that Russia needs to step up its efforts in countering 'fakes and trolls'.[40]

Russia may not be able to adopt a comprehensive firewall modelled on the Chinese example. It lacks the homegrown digital platforms that enable Chinese users to substitute foreign counterparts. Consequently, Russian Internet users are already all too reliant on foreign social media platforms and other online services. Still, Russia's move towards closer cooperation with China has triggered fears among liberal news outlets in Russia that it is moving closer and closer into that direction.[41] There are no illusions in Russia's relatively independent media outlets regarding the totalitarian nature of China's political regime and its control of the Internet, and these media have been consistently vocal that this is

---

ского интернета [Older comrade: Chinese censorship plan for the Russian Internet]. Retrieved from: https://republic.ru/posts/54061

[38] The Moscow Times. (2019). Chinese and Russian Cyber Watchdogs Meet in Moscow. Retrieved from: https://www.themoscowtimes.com/2019/07/18/chinese-and-russian-cyber-watchdogs-meet-in-moscow-a66465.

[39] Birger, P. (2015). Интернет-склероз: как будет работать закон о «праве на забвение» [Internet-Sclerosis: how will the law on the right to be forgotten work]. Retrieved from: https://republic.ru/posts/53432.

[40] RIA Novosti. (2019). Захарова рассказала о небылицах о Китае в российском интернете [Zakharova speaks about the fables about China in Russia's internet]. Retrieved from: https://ria.ru/20191011/1559667218.html.

[41] Kovachich, L. (2019). Китайский пример заразителен [The Chinese example is contagious]. Retrieved from: https://www.vedomosti.ru/opinion/articles/2019/01/28/792659-primer; Plyushchev, A. (2016). Комментарий: Российские теоретики учатся интернет-цензуре у китайских практиков [Russian theorists learn internet-censorship from Chinese practitioners]. Retrieved from: www.dw.com/ru/комментарий-российские-теоретики-учатся-интернет-цензуре-у-китайских-практиков/a-19222055.

something that Russia should not become.[42]

Perceived Cyber Espionage Originated from China

One particular sore spot in the Sino-Russian relationship, as it is in the Sino-American one, is economic espionage. Here, perhaps surprisingly, Russian experts share the perceptions and concerns of their Western counterparts. It is an established common understanding among Russian cybersecurity companies, scholars, and thinktanks that Russia's industrial, energy and research networks often experience cyberattacks from 'Chinese-speaking hackers'.

For Russia, the perceived IP theft by China is one of the main obstacles in the further deepening of mutual trust in cyberspace, even if Russia is presently not as outspoken as others about this issue[43]. According to Vladimir Lopatin, the Director of the Intellectual Property Department at the Russian Republican Centre for Intellectual Property, the prevailing practice of theft and illegal use of Russian intellectual property also led to a decline in the level of trust China has been able to gain from Russian research institutions and enterprises. This is a significant factor in restraining the implementation of strategic initiatives of innovative cooperation between the two countries. Moreover, it seems that the Chinese government lack(ed) incentives to commit to a bilateral agreement stating that both sides disapprove of commercial cybertheft. To add to Russia's frustration, China has already entered into such bilateral agreements with the US, the UK, and Germany.

There are well-founded suspicions in Russia that the Chinese government is closely associated with some of these cyberattacks. Russian cybersecurity company Kaspersky Lab, which is widely speculated to have extensive ties to the Russian government,[44] published an extensive report around the time Chinese president Xi Jinping visited Russia in 2017. However, it does not seem that the Kaspersky Lab's uncovering of covert cyber activities that seemingly originated from China has

[42] Republic. (n.d.). Китайский интернет — будущее России? [Is the Chinese internet the future of Russia?]. Retrieved from: https.

[43] Bendett, S. & Kania, E. (2019). A new Sino-Russian high-tech partnership, ASPI papers. Retrieved from: https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership.

[44] RBC. (2015). Bloomberg рассказал о связях Касперского с российскими спецслужбами [Bloomberg speaks about the connections of Kasperky Lab with the Russian special service]. Retrieved from:https://www.rbc.ru/politics/19/03/2015/550b02a29a79479cd82198d5https://www.rbc.ru/politics/19/03/2015/550b02a29a79479cd82198d5.

affected its cooperation with the Chinese security service and Huawei in the area of cybersecurity.[45] The report documented the activities of "Chinese-speaking" hackers in the third and fourth quarters of 2017 directed at Russian state projects with Asian countries. According the report China is also very interested in policies and negotiations involving Russia with other countries and observed three separate incidents where Russia and another country hold talks and are targeted shortly thereafter. For instance, in July, the campaign IronHusky targeted the Russian and Mongolian governments, aviation companies, and research institutes, after the two countries conducted talks related to modernizing the Mongolian air defences with Russia's help. In June, the energy sectors in India and Russia were targeted by 'Chinese-speaking hackers' after both countries signed a much-awaited agreement to expand a nuclear power plant in India, as well as further define the defence cooperation between the two countries. [46]

Cooperation in Digital Economy, on Paper?

The governments of China and Russia describe their relation as a 'comprehensive strategic partnership of coordination for a new era', and they have been undertaking more extensive technological cooperation in recent years, including in fifth-generation telecommunications, artificial intelligence (AI), biotechnology and the digital economy.[47] However, there are observations from both the Chinese and the Russian side that those co-operations usually remain initiatives agreed only at the senior leadership level, and often left unimplemented due to the lack of momentum from the academic and business sectors of both sides.[48] Besides, the call for Russia to participate in building the Digital Silk Road (DSR) also remained largely unanswered, due to conflicting geopolitical interest (for Russia) and the lack of profitability (for China). One particular sticking point for Russia and China to materialise the memoranda about Russia's participation in the DSR is the effect of secondary sanctions from the US, which punish persons and organisations that engage in business activities with Russian entities sanctioned by the US. Chinese companies are afraid to work with Russian partners that have close ties with the Russian government. Furthermore, what China needs

[45] Ye. A. Razumov. Dec 4 2020, personal communication.
[46] Kaspersky Lab. (2017). APT Trends report Q3 2017. Retrieved from: https://securelist.com/apt-trends-report-q3-2017/83162/.
[47] Bendett, S. & Kania, E. (2019). A new Sino-Russian high-tech partnership, ASPI papers. Retrieved from: https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership.
[48] RIAC & Fudan University. (2017). 中俄对话 [Sino-Russian Dialogue], p.17.

from Russia in an economic relation is Russia's natural resources, which China can acquire from Latin America and Africa without the risk of secondary sanctions.[49]

From the Chinese perspective, China hoped for more integration with the Russian-led Eurasian Economic Union (EEU), which has a moderately large consumer market but nascent native digital sector. Yet, it is only reasonable that Russia does not see this proposal as geoeconomically desirable, as it would make the EEU a market for Chinese goods.

In the area of digital economy, Russia sees itself as being in a vulnerable position: that it never had certain cutedge technologies, that Russia and the internal market of the EEU is small and cannot sustain on its own, and that Russia has limited resources to invest in new technologies.[50] Many Russian experts also agree that it is necessary to cooperate with China and leverage its capital and technology for the development of Russia, in terms of infrastructure, technology and investment. What Russia prefers, is to benefit from China's advantages in capital, and digital technologies (and its experience in the commercialisation of those technologies), and to attract Chinese investments and establish technological exchanges, without committing to more market access for Chinese tech-giants.[51] However, despite the abundance of official documents, regular meetings of officials and leaders of the two countries who emphasized the need to develop cooperation in the field of ICT, Sino-Russian exchanges between scientists, innovators, and businesses were until 2018, on one hand extremely small in scale, and on the other, devoid of any visible systematicity and depth.[52] China also rejected the vast majority of Russian projects under the flag of Belt and Road

[49] Falyakhov, R. (2019). Новый Шелковый путь: почему Россия остается на обочине [The New Silk Road: why is Russia still side-lined]. Retrieved from: https://www.gazeta.ru/business/2019/09/26/12684103.shtml.

[50] Danilin, I. (2020). Диалог России и Китая в сфере инновационных технологий [Dialogue of Russia and China in the sphere of innovative technologies]. RIAC Analytical Article. Retrieved from: https://russiancouncil.ru/analytics-and-comments/analytics/dialog-rossii-i-kitaya-v-sfere-innovatsionnykh-tekhnologiy/.

[51] RIAC & Fudan University. (2014). Диалог китая и россии 2014 [Dialogue of China and Russia - 2014], p.26.

[52] Danilin, I. (2020). Диалог России и Китая в сфере инновационных технологий [Dialogue of Russia and China in the sphere of innovative technologies]. RIAC Analytical Article. Retrieved from: https://russiancouncil.ru/analytics-and-comments/analytics/dialog-rossii-i-kitaya-v-sfere-innovatsionnykh-tekhnologiy/.

Initiative (BRI), citing unsustainable financial models and unclear prospects for returns.[53]

However, the recent intensification of US effort to contain China's high-tech sector changed this dynamic. Russia has started to evaluate the opportunities and risks for itself amid the ongoing Sino-American decoupling. Apart of this process, a new project initiated by RIAC in 2020, *Russia - USA - China: Protectionism, Security Issues and Competition in the Field of High Technologies*, researches the development of the Sino-American standoff and its implication for Russia.[54]

Most importantly, the Chinese strategy of cooperation with Russia in the field of ICT is ever more greatly dependent on the dynamics of Sino-American relations, according to the head of the Department of Science and Innovation of the IMEMO institute, another policy think tank originating from the Soviet era.[55] From the Chinese side, interest in cooperation with Russia is growing, and Chinese companies are beginning to develop more actively in Russia.[56] Inter alia, Huawei has recently opened an artificial intelligence laboratory in Moscow.[57] Contrary to the common perception about Huawei in the West, very few Russian scholars and experts

[53] Gabuev, A. (2017). Belt and Road to Where?. Retrieved from: https://carnegie.ru/2017/12/08/belt-and-road-to-where-pub-74957.

[54] RIAC. (2020). Проект: Россия — США — Китай: протекционизм, вопросы безопасности и конкуренция в сфере высоких технологий [Project: Russia – USA – China: protectionism, questions of security and competition in the sphere of advanced technologies]. Retrieved from: https://russiancouncil.ru/projects/functional/rossiya-ssha-kitay-protektsionizm-voprosy-bezopasnosti-i-konkurentsiya-v-sfere-vysokikh-tekhnologiy/.

[55] Danilin, I. (2020). Диалог России и Китая в сфере инновационных технологий [Dialogue of Russia and China in the sphere of innovative technologies]. RIAC Analytical Article. Retrieved from: https://russiancouncil.ru/analytics-and-comments/analytics/dialog-rossii-i-kitaya-v-sfere-innovatsionnykh-tekhnologiy/.

[56] Kashin, V. & Tolstukhina, A. (2020). Какие возможности открываются для России в условиях технологического противостояния США и Китая? [What opportunities does the technological confrontation between China and the US bring to Russia]. https://russiancouncil.ru/analytics-and-comments/interview/kakie-vozmozhnosti-otkryvayutsya-dlya-rossii-v-usloviyakh-tekhnologicheskogo-protivostoyaniya-ssha-i/.

[57] Danilin, I. (2020). Новый этап американо-китайской технологической войны: Huawei и другие цели США [New steps American-Chinese technological war: Huawei and other targets of the US]. RIAC analytical article. Retrieved from: https://russiancouncil.ru/analytics-and-comments/analytics/novyy-etap-amerikano-

believe that Huawei poses a cybersecurity threat to either Russia, or Europe.[58] Storchilov (2020) emphasises that despite the Western accusation against Huawei on creating backdoors for Chinese intelligence services to steal data from its users, there is not a single scandal where data of Huawei's users are actually leaked.[59] Furthermore, there are both regulatory and technical reasons for their confidence regarding the unlikelihood of cybersecurity threats caused by using foreign hardware in Russian infrastructure: in terms of regulation, Russia has adopted legislation to require smartphones and computers sold in Russia to install Russian operating systems. In terms of technicality, the incompatibility of technical specification of Chinese and Russian infrastructure further reduces the likelihood of cybersecurity threat from China.[60]

Similarly, Russian experts also believe that Huawei's recent difficulty in the West is only a result of the American effort to curb China's technological development and can only be reasonably understood in the context of the geopolitics of the Sino-American battle for technological supremacy. There are, however, contrasting views on whether Chinese tech-giants like Huawei will prevail in this battle, although most agree that it is yet too early to predict the victory of either side. For example, the director of RIAC, Ivan Timofeev, argues that Huawei is a company that is ultimately interested in maximising profit and will seek normalisation with the US. Like many other victims of US secondary sanctions, it is likely that Huawei will succumb to US demands.[61] Some other experts hold the view that Huawei fairly successfully circumvented US sanctions, and China will eventually succeed in the technological rivalry due to its ability to centralise efforts.[62]

---

kitayskoy-tekhnologicheskoy-voyny-huawei-i-drugie-tseli-ssha/.

[58] Ye. A. Razumov. Dec 4, 2020, personal communication.

[59] Storchilov, I. (2020). Позиция Huawei в сфере кибербезопасности [Position of Huawei in the sphere of cybersecurity]. Retrieved from: https://russiancouncil.ru/blogs/ilya_storchilov/35268/?sphrase_id=63595017.

[60] Ye. A. Razumov. 4 Dec.,2020, personal communication.

[61] Timofeev, I. (2020). От давления на Huawei американский бизнес проиграет [American business will lose from pressure on Huawei]. Retrieved from: https://russiancouncil.ru/analytics-and-comments/analytics/ot-davleniya-na-huawei-amerikanskiy-biznes-proigraet.

[62] Danilin, I. (2020). Новый этап американо-китайской технологической войны: Huawei и другие цели США [New steps American-Chinese technological war: Huawei and other targets of the US]. RIAC analytical article. Retrieved from: https://russiancouncil.ru/analytics-and-comments/analytics/novyy-etap-amerikano-kitayskoy-tekhnologicheskoy-voyny-huawei-i-drugie-tseli-ssha/.

Nevertheless, in a scenario of complete decoupling between the United States and China, where two technological ecosystems incompatible with each other are created, Russia will have to make a choice between the US and China. One authoritative author even called for Russia to form a technological ecosystem with Europe.[63] Maybe it is indeed wishful thinking, but increasing connectivity and technological synchronisation with the EU is considered to be a way to reduce the risk of Sino-American decoupling.[64] Even in a milder scenario of Sino-American tech-standoff, it still remains a question among Russian experts to what extent Russian regulators should allow Russian companies to be included in Chinese-dominated value chains in order to best suit Russian interests – it is a tricky balance between isolation from the global digital economy and becoming China's junior partner and a market for Chinese digital goods and services.[65]

Conclusion and Recommendations

Although Western observers often lump China and Russia together as authoritarian states hostile to the status quo in cyberspace, and as the core of a coalition of adversaries, the extent of their collaboration remains limited, and there are considerable concerns in Russia about Chinese actions and policies, as well as with greater integration with Beijing. While the relationship is close at the senior leadership level, initiatives at the working level are often more limited, especially in the economic sphere, and rarely lead to sustained implementation of plans and initiatives. Even so, there are indications that perceived hostility from the West, most notably the US, are pushing both countries closer together. Conversely,

[63] Matveenkov, K. (2020). На грани развода. Куда приведет технологическая война между Китаем и США? [On the verge of divorce. Where will the technology war between China and the United States lead?], RIAC Analytical Article. Retrieved from: https://russiancouncil.ru/analytics-and-comments/analytics/na-grani-razvoda-kuda-privedet-tekhnologicheskaya-voyna-mezhdu-kitaem-i-ssha/.

[64] Danilin, I. (2019). США и Китай: война за статус технологического лидера [USA and China: war for the technological leadership]. Retrieved from: https://russiancouncil.ru/analytics-and-comments/interview/ssha-i-kitay-voyna-za-status-tekhnologicheskogo-lidera/.

[65] Afontsev, S. (2020). Воздействие американо-китайского «расцепления» на мировую экономику и риски для России [Impact of the US-China "decoupling" on the global economy and risks for Russia], RIAC Analytical article, Retrieved from: https://russiancouncil.ru/activity/policybriefs/vozdeystvie-amerikano-kitayskogo-rastsepleniya-na-mirovuyu-ekonomiku-i-riski-dlya-rossii/.

Russian and Chinese cyber operations, combined with increasing political repression in both countries, have drastically reduced the appetite for engagement in European capitals. In the Chinese case, recriminations surrounding the COVID-19 pandemic have exacerbated this problem.

Even so, the question of how to find some degree of accommodation and cordial coexistence with both countries will remain. In conducting the creative thought process that will be necessary in this process, it helps to step away from the widely accepted but simplistic binary between the West and its adversaries. Russia and China are likely going to remain non-liberal democracies for the foreseeable future, and therefore policy should not be based on the notion that they might be. This means that a grand bargain, or the sort of overall cyber treaty China and Russia pursue, will be nearly impossible to achieve. Yet in the meantime, some modus vivendi needs to be found on specific issues, in what will probably result in a patchwork of specialized agreements and practices. Knowing where Russian and Chinese interests converge and diverge, as well as where their relative strengths do and do not lie is very important in this regard, as well as to forecast possible reactions to proposals or policy developments. A last point is that this report makes clear that the level of domestic consensus and coordination of opinions and resources in Russia is low. This constrains the Putin administration's space for action in various ways, including with regard to China.

This report is published by the LeidenAsiaCentre.

Eric Siyi Zhang is a research assistant at the LeidenAsiaCentre. His main research interests are cyber security and disinformation, with regional focuses on China and Eastern Europe.

Dr Rogier Creemers is an assistant professor at Leiden University's China Studies department. His main focus of research is the development of Chinese policy in the digital sphere, both domestically and at the global level.

This report forms part of the China in Global Cyberspace project, funded by the Netherlands Ministry of Foreign Affairs.