A coalition of the unwilling? Chinese and Russian perspectives on cyberspace

Broeders, D.W.J.; Adamson, L.; Creemers, R.J.E.H.

2019 Policy brief

A coalition of the unwilling?

Chinese & Russian perspectives on cyberspace

Dennis Broeders, Liisi Adamson and Rogier Creemers

THE HAGUE PROGRAM for Cyber Norms

LEIDEN ASIA CENTRE

Universiteit Leiden

Suggested citation:

Broeders, D., L. Adamson and R. Creemers. (2019).
Coalition of the unwilling? Chinese and Russian perspectives on cyberspace.
The Hague Program For Cyber Norms Policy Brief. November 2019.

A coalition of the unwilling? Chinese and Russian perspectives on cyberspace

Introduction

China and Russia have distinct views on the global order and the role of cyber therein, expressed in a conceptual vocabulary that has received little scholarly attention. This vocabulary is also used to frame their concerns and fears about cyber-borne threats. The approaches and policies of Russia and China are often married together under the heading of “the Sino-Russian approach”. This rings true not only in cybersecurity and -defence related discourse, but in West vs. East geopolitics in general. The Sino-Russian approach is often contrasted to the Western or “likeminded” approach, which represents the liberal world order. At the same time, little attention has been paid to the question, how united this Sino-Russian front is. Is it “us against the world”? Is the Sino-Russian approach “likeminded” in its grouping? Or are there discrepancies in this united front? Having a one-dimensional view of the Chinese-Russian relationship and omitting the different motives and goals of both actors undermine the intricacies and possibilities that a deeper understanding of the cyberspace-related policies of both countries might bring to western analysts and policy makers.

In order to explore aspects of the Sino-Russian relationship in cyberspace, The Hague Program for Cyber Norms and the Leiden Asia Centre convened a dozen experts for a workshop in The Hague in May 2019. The experts were all from Europe and North America focusing on China or Russia – sometimes both – and most of them focused on aspects of foreign policy and/or cyberspace. The workshop was held under Chatham House rule.

China’s and Russia’s attitudes towards global cyber affairs: translation and peculiarities

Both the Chinese and the Russian worldview share a rejection of the current rules-based liberal world order, which they perceive as a project of Western hegemony, even if they disagree on the exact nature of the change they would like to see. They also share a historical family resemblance based on Leninist ideas of state control, where a single unified political actor is in overall charge of the entire system and information channels must be controlled by the state. They agree, at least rhetorically, on the fundamental importance of sovereignty and non-intervention in intergovernmental cyber affairs and share a focus on the potential harm originating from online content and information. Nonetheless, there are also important differences between both countries’ approaches, often stemming from differing national interests and policy styles, as well as perceptions about the respective global position of each. This section will address the origins of these similarities and differences.

The most important point of agreement between Beijing and Moscow is their distrust of the Western 'liberal order', which they perceive as a US-led, hegemonic attempt at global dominance and potential regime subversion. In Russia, this distrust stems from the country's experience after the end of the Cold War. The dissolution of the Soviet Union significantly reduced Russia's importance in global security affairs, and its superpower status. Russia today has roughly half the population and three quarters of the territory of the former Soviet Union.[1] The eastward expansion of NATO and the European Union have caused resentment about the decline of Russia's sphere of interest, as well as traditional export markets for Russian goods. China, on the other hand, perceives the United States as an existential threat that intends to "divide and Westernize"[2] the country, curtailing China's resurgence to justified great power status.

Because of similarities in national interests and ideological outlook, both countries share a largely common vocabulary when it comes to cyber issues. Seeing cyberspace as an extension of real space, instead of a *sui generis* phenomenon, they primarily focus on "information security" rather than cyber security. While they use technological means to defend this information space, they seek to establish the norm of "cyber sovereignty" in global politics, providing legal underpinnings against perceived foreign interventions. Under this definition, cybercrime is defined more broadly than in the West, covering not only matters such as drug trade, fraud and child pornography, but also subversion and separatism, often dubbing this "terrorism" or "extremism". Both countries advocate the "peaceful use" of cyberspace, meaning it should not be used for military purposes, similar to outer space. In response to external threats, both countries claim the right to use "active defence".[3] Nevertheless, there are two important differences. First, unlike Russia, China has also developed a positive conceptual framework concerning global cyberspace. The concept of a "community of common destiny in cyberspace" may be a counteraction to the American-led Internet freedom agenda, but it envisages a degree of international cooperation that seems absent from Russian thinking. Second, the differing centre of gravity in both countries' cyber policies means these terminologies are often interpreted and implemented in differing ways. Military and intelligence matters, at least for the time being, are relatively less important for Beijing than they are for Moscow.

In cyberspace, both countries see online information as the primary risk. China has long voiced concerns about "foreign hostile powers" using media and propaganda tools for ideological subversion and regime change.[4] In response, it has erected and gradually enhanced filtering capabilities for foreign content, generally known as the Great Firewall of China. By now, this filters a range of foreign news media websites and political content, as well as social media platforms that China deems complicit in the Arab Spring and a series of colour revolutions. The great firewall

[1] Richard Ellings. (2018). "The Strategic Context of China-Russia Relations", pp. 3-48 in: Richard Ellings & Robert Sutter (eds.). (2018). *Axis of Authoritarians: Implications of China-Russia Cooperation.* Washington, DC: The National Bureau of Asian Research (NBR), p. 25.

[2] See, for instance: Rogier Creemers (ed.). (2012). "Hu Jintao's Article in Qiushi Magazine – translated". *China Copyright and Media,* 4 January 2012.

[3] The State Council Information Office of the People's Republic of China. (2015). *China's Military Strategy,* May 2015; Ministry of National Defense of the People's Republic of China. (2019). *China's National Defense in the New Era,* July 2019.

[4] Hu Jintao. (2011). "Jiandingbuyi zou Zhongguo tese shehuizhuyi wenhua fazhan daolu [Resolutely walk the path of Socialist culture development with Chinese characteristics]." In: "Hu Jintao's Article in Qiushi Magazine – translated". *China Copyright and Media,* 4 January 2012.

supplements the very strict censorship of the domestic (social) media ecosystem. Russia has over the past two decades developed an information security doctrine integrating traditional security notions and shares Chinese concerns about foreign propaganda and colour and twitter revolutions. In recent years, Russia has also demonstrated increased interest in developing similar filtering tools, borrowing some of China's approaches and concepts.[5]

In the field of international law, both countries have strongly advocated the notion of cyber sovereignty, contained amongst others in the two Codes of Conduct they have proposed at the UN General Assembly.[6] Cyber sovereignty entails that national governments have exclusive power of jurisdiction over their own national cyberspace at the level of both infrastructure and content. Moreover, they do not merely see this as a point of international law leading to particular legal rights and entitlements *de jure,* they have both taken steps to develop the industrial and security capacity to ensure sovereignty *de facto.* In this area, China has made greater progress, owing to the relative strength of its digital sector. This stance on sovereignty reflects misgivings about the US' reading of international law, which claims to make state sovereignty conditional on respect for universal fundamental rights[7]. In response, Russia takes a quite positivist approach to international law, pushing for a new cyber treaty that would lay down specific rules for cyberspace. From the Russian perspective, this legalist approach not only serves to bind its counterparts, it is also an aspect of Russian influence projection. China has taken slightly less initiative in international law, preferring to leverage Russia's greater experience, particularly in the UN realm. This does not mean it opposes the application of international law in cyberspace. Rather, Beijing is hesitant to commit to a reading of international law that does not equally bind its most important adversary.

Perhaps the most important differences between both countries are the relative importance of the technological industry, and relatedly, their long-term geopolitical outlook. China is deploying a cyber-power *(wangluo qiangguo)* strategy.[8] This strategy integrates informatisation, or the build-up of a technology industry and digitally empowered government, with cybersecurity. Chinese businesses have become global leaders, and China intends to further gain global leadership in emerging and core technologies such as artificial intelligence and semiconductors. Partly, the objective is to further China's ascent up the economic value chain, but increasingly, it is also attempting to reduce a perceived vulnerability of overreliance on American technology. Export markets are seen as key in this regard, as evidenced by the rapidly growing digital component of the Belt-Road Initiative (i.e., digital silk road)[9]. Moreover, the increasing integration

[5] Alex Hern & Marc Bennetts. (2019). "Great Firewall fears as Russia plans to cut itself off from internet". *The Guardian,* 12 February 2019

[6] "International code of conduct for information security (2011)", in: United Nations General Assembly. (2011). "Letter dated 2011/09/12 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", UN Document A/66/359, 12 September 2011; "International code of conduct for information security (2015)", in: United Nations General Assembly. (2015). "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General". UN Document A/69/723, 9 January 2015.

[7] See, for instance, Yang Runguang. (2013). "Understanding the US Human Rights View and Human Rights Practice [translation]". *China Copyright and Media,* August 2013.

[8] Rogier Creemers et al. (2018). "Lexicon: 网络强国 Wǎngluò Qiángguó". *New America*, 31 May 2018.

[9] Tin Hinane El Kadi. (2019). "The Promise and Peril of the Digital Silk Road", *Chatham House – Expert Comment,* 6 June 2019. London: Chatham House, The Royal Institute of International Affairs.

of network technology with traditional industries intimately connects China's whole-spectrum economic development plans to success in the digital environment. Chinese success in growing domestic and international technology companies also makes the global operators among them, such as Huawei, ZTE and Alibaba, more vulnerable to international political push back. Consequently, China's tech businesses wish to maintain access to and interoperability with global cyberspace, offsetting some of the more hawkish attempts to increase separation. Russia, on the other hand, has a less elaborate approach to the use of technology in domestic governance, and less of a corporate stake in the development of the global digital economy. This means that where both countries do seek to change the nature of the international political order, China is far more invested in the stability of its economic aspects.

Another important difference does not concern worldviews or ideologies, but the extent to which both countries have deployed cyber operations in pursuit of national objectives. Russia seems to pursue a policy of political destabilization of Western countries, with the 2016 US presidential election and Brexit being the two best known of numerous influence operations based on spreading fake news and trolling through social media.[10] Chinese hackers, on the other hand, have mostly concentrated on economic targets, in pursuit of valuable intellectual property or sensitive business information[11]. There are, however, a few exceptions to these trends, which are primarily concerned with what China identifies as core national interests. The Great Cannon attack, attributed to China, aimed to paralyse GitHub, a coding platform containing, amongst others, software to circumvent the Great Firewall.[12] It was also alleged that China sought to interfere in the 2018 elections in Taiwan[13], and Facebook and Twitter closed a number of ostensibly China-run accounts spreading disinformation during the 2019 Hong Kong protests[14].

Neither China nor Russia has ever publicly admitted to cyber operations they allegedly committed. Nevertheless, it is quite clear how they can be justified within their respective worldviews. China, seeking economic development and political stability, has combined a politically defensive stance with cyber activities serving to enhance economic capabilities and competitiveness with the United States.[15] Russia, with its more limited economic interests and a greater influence of military and intelligence services, is applying its information security doctrines against external targets in order to effect political destabilization and paralysis. Yet its preferred endgame is less clear than China's, and its chaos-based tactics more prone to escalation and unintended consequences.

[10] Peter W. Singer & Emerson T. Brooking. (2018). *LikeWar: The Weaponization of Social Media.* New York: Houghton Mifflin Harcourt Publishing; Andrei Soldatov & Irina Borogan. (2018). "Russia's approach to cyber: the best defence is a good offence", pp. 15-23 in: Nicu Popescu & Stanislav Secrieru (eds.). (2018). *Hacks, leaks and disruptions: Russian cyber strategies.* Chaillot Paper 148, October 2018. Paris: EU ISS.

[11] National Counterintelligence and Security Center (US). (2018). *Foreign Economic Espionage in Cyberspace*.

[12] Bill Marczak et al. (2015). "China's Great Cannon". *The Citizen Lab,* 10 April 2015.

[13] Paul Huang. (2019). "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate", *Foreign Policy,* 26 June 2019.

[14] Kate Conger. (2019). "Facebook and Twitter Say China Is Spreading Disinformation in Hong Kong". *The New York Times,* 19 August 2019.

[15] Samm Sacks. (n.d.). "China's Emerging Cyber Governance System". Center for Strategic and International Studies.

The bilateral relationship: façade and reality

Whereas Russia and China are on the global scale often seen as a united front, sharing a strong family resemblance in their general worldviews and how they identify threats, concerns, concepts and opportunities in cyberspace, less attention has been paid to their bilateral relationship, especially in matters of cyberspace. Three elements are of importance. What is the degree of actual bilateral cooperation, or the lack thereof? How do relations with third countries in each other's influence sphere influence Sino-Russian relations? And lastly, how do cyber operations targeting third parties affect bilateral relationships?

Bilateral cooperation or lack thereof

Sino-Russian cooperation is much closer, especially in military and economic terms, than it has been in decades, even if much of it is fragmented and not well embedded institutionally.[16] China is the single largest trading partner for Russia. However, Russia only ranks 12th for China.[17] On the military cooperation front, Russia recently included PLA troops in its latest military exercise *Vostok* in 2018.[18] Furthermore, in July 2019 China and Russia conducted a joint air patrol in the Asia-Pacific in order to increase the cooperation of armed forces and improve their capabilities to carry out joint actions.[19] In the cybersecurity realm, China and Russia concluded a bilateral information security treaty in 2015,[20] outlining major threats and vectors of cooperation in cyberspace. Both of them continue to work under the auspices of the Shanghai Cooperation Organization (SCO), as founding members, with issues of security, including *inter alia* information security. Furthermore, there are currently no serious disputes among the two and they share a similar focus on regime security, which supersedes or is on par with national security, and which underpins their joint interest in controlling the (national) information sphere. Russian authorities announced the conclusion of a Sino-Russian agreement with treaty status on governing online content in October 2019[21]. However, under the surface of this united front, there are significant dissimilarities and asymmetries.

The harmonious Sino-Russian front might be a façade of sorts. Whilst the international community can see an alignment of certain values among the two countries, this is not necessarily a coherent alliance with aligned actions and goals. An indicator for this is also the fact that while this coherent front exists on the highest level – between Vladimir Putin and Xi Jinping – it is hard to assess what

[16] Thomas Ambrosio. (2017). "The Architecture of Alignment: The Russia–China Relationship and International Agreements". *Europe-Asia Studies,* 69 (1): pp. 110-156.

[17] World Bank. "China exports, imports and trade balance – By Country – 2017". *World Integrated Trade Solution (WITS).*

[18] Minnie Chan. (2018). "Vostok 2018 war games: China's chance to learn Russia's military lessons from Syria". *South China Morning Post,* 29 August 2018.

[19] Andrew Osborn & Joyce Lee. (2019). "First Russian-Chinese air patrol in Asia-Pacific draws shots from South Korea". *Reuters,* 23 July 2019.

[20] *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.* (2015). Original and translated version can be found in: "Sino-Russian Cybersecurity Agreement 2015". Center for Strategic & International Studies, 11 May 2015.

[21] "China and Russia to sign treaty aimed at combating illegal internet content". *South China Morning Post,* 9 October 2019.

cooperation exists on the working and operational level.[22] For example, both of them do not partake in each other's major projects. Russia has been counting on China joining its cybercrime initiative, yet thus far, that support has not materialized. In many economic areas, other than natural resources, China's investment in Russia is lagging behind original promises.[23] Also, the vast majority of Russian proposals for cooperation under the Belt and Road Initiative (BRI) have been rejected by China.[24] China, in turn, has been silent on the announced content control agreement with Russia. These could be minor indications that the differences in global economic and geopolitical outlook contain fault lines that could lead to greater tensions or rupture in the future.

Bilateral relations and zones of influence

Another potential point of contention is that the expansion of global Chinese power projection encroaches on the traditional Russian sphere of influence, which already shrank tremendously in the wake of the demise of the USSR. China is increasingly replacing Russian influence in Eastern Europe, mostly through investments, competing with Russian historical – but waning – influence in the region. In 2012 China initiated a cooperation initiative with Central and Eastern Europe (China + CEE, 17+1) focusing on economic and investment cooperation.[25] For example, China is the second largest investor in Ukraine. China employs outreach projects as a strategy to affirm its foothold as a global power. In doing so it expands into other traditional zones of Russian influence. China is expanding into Africa not in the least in terms of providing digital infrastructure for states and international organisations such as the African Union. These create dependency on Chinese technology, pave the way for Chinese emerging global infrastructure in the region, such as 5G, and sometimes open them up to Chinese digital espionage.[26] The Belt and Road Initiative (BRI) cuts through the traditional Russian influence sphere in central Asia. For now, this is tolerated by Russia as it projects Chinese economic power rather than constituting a military presence. However, the Belt and Road Initiative is increasingly likely to expand into military matters as growing Chinese regional interests may require safeguarding. The recently established military base in Djibouti may thus be a precursor to greater military presence and projection. Managing good Sino-Russian relations in this geographical area may come under pressure as Chinese geopolitical ambitions grow and BRI incorporates more elements of international security and international power projection.[27] Lastly, BRI goes through the Middle East into Europe, crossing through a Russian 'near abroad' that is vital to Moscow in terms of geopolitical interest, and in terms of being a global supplier of gas and fossil fuels, which is one of the main underpinnings of the Russian economy. Chinese success in this field, by projecting economic soft power may become a future point of friction in the Sino-Russian relationship.

[22] The united front at the top level of president Xi Jinping and president Vladimir Putin is out of sync with some of the lower operational and working levels, where cooperation is essential. See for example: Frederick Kempe. (2019). "Special edition: Xi and Putin's budding bromance". Atlantic Council, 1 June 2019; Moritz Pieper. (2018). "Mapping Eurasia: Contrasting the Public Diplomacies of Russia's 'Greater Eurasia' and China's 'Belt and Road' Initiative". *Rising Powers Quarterly,* 3 (3): pp. 217-237; Saibal Dasgupta. (2019). "Putin Demands a Role in Eurasian Part of Belt and Road". *Voice of America,* 4 May 2019.

[23] Dmitri Trenin. (2012). *True partners? How Russia and China see each other*. London: Centre for European Reform, February 2012, p. 34.

[24] Alexander Gabuev. (2017). "Belt and Road to Where?". Carnegie Moscow Center, Council for Security Cooperation in the Asia Pacific, 8 December 2017.

[25] *Cooperation between China and Central and Eastern European Countries.* (2013-2015).

[26] As happened in the case of the African Union Headquarters that were built by China. See: Mailyn Fidler. (2018). "African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts". *Net Politics,* Council on Foreign Relations, 7 March 2018.

[27] Richard Weitz. (2018). "Growing China-Russia Military Relations: Implications and Opportunities for U.S. Policy", pp. 81-106 in: Richard Ellings & Robert Sutter (eds.). (2018). *Axis of Authoritarians: Implications of China-Russia Cooperation.* Washington, DC: The National Bureau of Asian Research (NBR), pp. 83-84.

Divergences

Furthermore, clearly the partners do not endorse everything the other does, and that goes especially for the cyber domain. China's own approach to cybersecurity would suggest that China does not approve of Russian cyber operations pertaining to election interference or attacks on critical infrastructure, but Beijing does not openly call out Moscow. As Russia challenges the international order in an increasingly heated and explosive manner, China is distancing itself from such actions, as it is not interested in the chaos that Russia wants to create. For example, China has not recognised the annexation of Ukrainian or Georgian territories, but it recognises the historical complexities accompanying such situations.[28] Thus, whereas Russia has actively pursued destabilization abroad, China is more interested in strategic stability and predictability. Also, the international community's reaction to cyber-attacks perpetrated by China or Russia varies greatly, not in the least as a result of the targets they choose. For example, the reaction to the OPM hack in the US was relatively subdued, with high-level American intelligence officials declaring it 'honorable espionage'.[29] Other cyber operations – especially those involving economic espionage – perpetrated by Chinese received more pushback and resulted in international naming and shaming and individual criminal indictments.[30] However, the backlash after cyber operations perpetrated by Russia, for example targeting Ukraine (in violation of international law as well as peacetime UN GGE norms) and US elections, has been much more intense, leading even to international public attributions as in the case of NotPetya.[31] As these were attacks against critical infrastructure and integrity of data, they were perceived as much more serious than the availability and confidentiality attacks generally seen from the Chinese side. In recent months, however, the rapidly developing tensions in the overarching relationship between China and the US have predominantly manifested themselves in the areas of technology and trade, meaning questions around cyber have become embedded in a broader and more volatile evolution.

In sum

It seems clear that the bilateral relationship is more important to Russia than China. China's increasingly global strategy has resulted in the rapid expansion of Chinese power, which has caused a growing inequality in the bilateral relationship as well. Russia has countered this with strategic flexibility where necessary, for example by accepting Chinese activities in traditional Russian spheres of influence. With the understanding that Russia will not likely actively help China achieve its goals, the asymmetric partnership is acceptable to China as long as Russia's actions will not hinder the (economic) progress it wants to make. Thus, a more fundamental divergence may emerge, especially when Russia's disruptive actions start to harm Chinese interests. Russia's approach is more reactive and disruptive vis-à-vis the current world order than China's more incremental vision. China focuses more on economy as a force multiplier for global power projection in cyberspace and beyond, banking on patience and the waiting game.[32]

[28] Zhang Lihua. (2015). "Explaining China's Position on the Crimea Referendum". Carnegie–Tsinghua Center for Global Policy, 1 April 2015.

[29] Damian Paletta. (2015). "Former CIA Chief Says Government Data Breach Could Help China Recruit Spies". *The Wall Street Journal,* 15 June 2015.

[30] Garrett Hinck & Tim Maurer. (2019). "What's the Point of Charging Foreign State-Linked Hackers?". *Lawfare,* 24 May 2019.

[31] White House. (2018). "Statement from the Press Secretary", 15 February 2018; Government of Canada. (2018). "CSE Statement on the NotPetya Malware", 15 February 2018; Australian Government. (2018). "Australian Government attribution of the 'NotPetya' cyber incident to Russia", 16 February 2018; New Zealand Government. (2018). "New Zealand joins international condemnation of NotPetya cyber-attack", 16 February 2018; United Kingdom Foreign Office. (2018). "Foreign Office Minister condemns Russia for NotPetya attacks", 15 February 2018.

[32] See also: Marcin Kaczmarski. (2019). "Convergence or divergence? Visions of world order and the Russian-Chinese relationship". *European Politics and Society,* 20 (2): pp. 207-224.

Sino-Russian cooperation on the world stage

It is on the international stage that China and Russia often seem a united front. Yet, the differences between their views of the global order and their interests also manifest themselves in their cooperation in international cyber affairs. This plays out in three key areas. Firstly, while their resistance to American global dominance unites them, they do not share an identical vision of what a future global order should look like. Secondly, this plays out in their diplomatic relation and (shared) agenda, as well as, thirdly, in military relations and their respective versions of projection of cyber power.

Visions of the future world order

Perhaps the biggest point of contention in the Sino-Russian relationship is their long-term vision of what the world order should look like. China and Russia see the current liberal world order as hegemonic and built on American exceptionalism. Both countries agree that a new world order is needed that reflects their status as great powers. Moreover, their issue with the liberal order is with the political (liberal democracy, freedom of speech) rather than the economic aspects of the model. However, the Russian view of the current world order is almost entirely negative, picturing the international order as an order in terminal demise, convinced that this decline ought to be expedited. It follows, as Keir Giles argues, that practical cooperation with Russia is only possible if issues are 'ring-fenced' and based on renouncing the western 'hope that Russia will, after all, in the end turn out to think just like the West does'.[33] China, on the other hand, seeks to reform, not destroy the international system[34]. As China has been a prime beneficiary of the liberal world order, maintaining a functional relationship with the US as well as being the architect of the future reform are important priorities. Furthermore, even though both countries share a sense of opposition to the hegemony of the West, Chinese traditional sense of identity is not necessarily anchored to the West as a historical reference.[35] The same does not hold true for Russia, who sees the liberal West inherently and historically as a competitor, while simultaneously seeing itself as a European power. Thus, their vision for enhancing their power is a question of confrontation versus accommodation. It follows that even though changing the liberal order is a shared ambition, *disrupting* it is not necessarily a joint goal of China and Russia.

Both countries' views on the future world order reveal a major rift: where Russia envisions a new world order of three great powers, with Russia in a crucial intermediary role, China ultimately envisions a bi-polar order with China on a par with the US.[36] In the end, these visions are irreconcilable and a source of tension between the two countries. At what point this may

[33] Keir Giles. (2019). *Moscow Rules: What Drives Russia to Confront the West.* London: Brookings Institutions Press/Chatham House, p. 171.

[34] National Counterintelligence and Security Center (US). (2018). *Foreign Economic Espionage in Cyberspace;* House of Commons, Foreign Affairs Committee. (2019). *China and the Rules-Based International System: Sixteenth Report of Session 2017-2019,* 4 April 2019, pp. 8-13.

[35] Aldo Ferrari & Eleonora Tafuro Ambrosetti (eds.). (2019). *Russia and China: Anatomy of a Partnership*. Milano: ISPI, p. 20.

[36] Yan Xuetong. (2019). "The Age of Uneasy Peace: Chinese Power in a Divided World". *Foreign Affairs,* January/February 2019, pp. 40-46.

outweigh the strategic usefulness of their current alliance is hard to say, but their respective approaches to regime change will play an important role in this. Russia is more confrontational and disruptive, seeking mostly acknowledgement of its (military) great power status, similar to the days of the Cold War. China is more transformative: seeking a change of the system that reflects the rising position of China. Beijing is also more fearful of breaking the current order when there is no alternative in place. Anarchy is not a good replacement for the model that has been instrumental in China's rise to economic power.

Thus, to an extent this classic balance of power exercise shows that even though their common ground is rooted in their respective national interests,[37] cooperation may come under duress when the generalist and specialist approaches of China and Russia, respectively, clash. It follows that it is a common goal of Russia and China to protect the national information sphere from outside interference.[38] Their push for (digital) sovereignty and upholding the principle of non-intervention serves as a diplomatic shortcut to protect not only the information sphere, but also to safeguard regime stability. Yet, where the latter, alongside projection of power, is the main concern for Russia, there is an additional calculus for China in play. China is a rising economic superpower with high global ambitions in the digital economy. Chinese internet and artificial intelligence companies ranking in the global corporate top 10 and the global geopolitical battle over 5G are illustrations of Chinese ambitions in providing global internet infrastructure. Here, economic prowess is one of the core characteristics of China as a cyber-power. Russia, however, does not claim a stake in the global internet economy as a top-tier player. Instead, it seems to be more focused on aggressive, below the threshold, covert, and disruptive cyber-presence. Thus, while the high-level cooperation between the countries might be apparent, when the underlying calculus differs, rifts may emerge.

The asymmetric strengths and expertise that both sides bring to the table in the bilateral relationship are useful for now and serve their interest for the projection of power.[39] It is unlikely that this unity will prevail when their national interests diverge, or when one starts to undermine the others' interests. Here, the deck seems stacked in favor of China, which is the rising power. Russia depends more on China for its international role than vice versa and this asymmetry might grow over time. China is also playing for time: it feels it still lags far behind its major competitor and will be in a better position to meet future challenges with every passing day. This does not necessarily apply to Russia.

[37] Hence, interpreting the apparent cohesion of this relationship as an axis of authoritarianism versus the Western liberalism could be misleading. It is more so an asymmetrical strategic partnership of convenience that is carried by different strengths and national interests pertaining to geopolitics and power, economy and normative order.

[38] Russian fear and suspicion of the Internet has centered on the issue of information security since 1998 and China shares this concern. See: United Nations General Assembly, "Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary- General" A/C.1/53/3, 1998.

[39] Russia brings to the table expertise in geopolitics and diplomatic capabilities (including cyber diplomacy), honed historically through different technological developments from space to nuclear technologies. Yet, it is often portrayed as the declining power that does not have a big picture, long-term strategy for maintaining power. China, being a rather new, but economically strong actor, is increasingly perceived as a global power that is oriented to greater spectrum preponderance. Whilst diplomacy is the strong suit of Russians, Chinese strengths pertain to economic issues and trade, especially in the WTO.

Diplomatic relations

In the diplomatic arena China can be seen as operating under the shelter of the Russian position at times. Russia's defiance and disruptive nature can serve as a heat shield allowing China to abstain when it is sure of a Moscow veto.[40] It follows that Russia often absorbs the heat as the worst offender covering to an extent for China and its lesser infringements. For example, the Chinese land reclamation projects in the South China Sea took place in the shadow of Russian operations in Crimea and Donbass. This is strategically convenient for China. In other parts of the diplomatic arena – outside of the cyber domain – China has been stepping forward, for example in countering climate change and supporting peace keeping missions. When it comes to the normative challenges of cyberspace, China and Russia both agree on the need for a new cyber specific multilateral solution to govern cyberspace, i.e. ideally a cyber-treaty, that would emphasise the importance of sovereignty and information control, as well as provide a more equitable form of global governance of the internet and the global digital economy. Domestically, the recent developments of Russia adopting laws to create RusNET[41] alongside the already established data localisation laws show efforts to move in that direction. Similarly, a new Chinese draft regulation on data traffic mandates that all Chinese traffic should be routed domestically.[42] The emphasis on sovereignty and information security is witnessed also in the bilateral treaty on information security concluded in 2015. Yet, the global discussion on a new treaty has never gained serious international traction. The Codes of Conduct both countries presented (in 2011 and 2015)[43] to the UN, jointly developed under the aegis of the Shanghai Cooperation Organization, never received broad endorsement.

Their vision of great power politics also influences the way they see international law and multilateral normative efforts. International law is an instrument of (great) power projection rather than a tool that binds all states equally. To Russia, sovereignty and independence are qualified concepts. Only great powers can be truly sovereign, smaller and less powerful states are under the influence of more powerful states.[44] China sees the world similarly, illustrated acutely by Foreign Minister Yang Jiechi's 2010 quip that "China is a big country and other countries are small countries, and that's just a fact".[45] This is inspired by a long history of great power exceptionalism, currently exemplified by the US, which both Russia and China consider to be a habitual norm breaker. Great power status is intertwined with exceptionalism and both countries (will) apply this to themselves as their global position increases. Thus, *shaping* and *creating* international law and norms is perceived to be the work of great powers. To be a leading, responsible nation is to negotiate treaties and shape the international order. The experts in the workshop suggested that for Russia the façade of being seen to shape the international environment holds more power than for China, that wants to shape the substance of the new order.

[40] For example, in the context of the UN Security Council.

[41] Zak Doffman. (2019). "Putin Signs 'Russian Internet Law' To Disconnect Russia From The World Wide Web". *Forbes,* 1 May 2019.

[42] Katharin Tai et al. (2019). "Translation: China's New Draft 'Data Security Management Measures'", *New America,* 31 May 2019.

[43] United Nations General Assembly. (2011). "Letter dated 2011/09/12 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General". UN Document A/66/359, 12 September 2011; United Nations General Assembly. (2015). "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General". UN Document A/69/723, 9 January 2015.

[44] Keir Giles. (2019). *Moscow Rules: What Drives Russia to Confront the West.* London: Brookings Institutions Press/Chatham House, p. 27.

[45] Ben Lowsen. (2018). "China's Diplomacy Has a Monster in its Closet". *The Diplomat,* 13 October 2018.

In the cyber domain, the prime diplomatic venue for discussing responsible state behavior at the global level has been the UN Group of Governmental Experts (UN GGE). Russia brought the issue of the potential threat of ICTs to international peace and security to the UN in 1998, calling for the negotiation of a cyber-treaty, but was rebuffed by most of the Western states on that point. The UN GGE process – which is non-binding – was started up later to create a venue at the UN level for deliberation of the issue without going down the road of a treaty.[46] Russia and China, as permanent members of the Security Council, have participated in all rounds of the UN GGE. In three iterations of the process (out of five) the group of experts produced a consensus report, with as main yields the principle that International Law applies in cyberspace and the formulation of a number of non-binding norms for responsible state behavior in the 2015 consensus report.[47] After the 2017 round of the UN GGE failed to achieve consensus, there were many reports of the "death of the norms process",[48] but in November 2018 the UN General Assembly voted on two parallel and competing resolutions. The first was submitted by the US and supported by western states – often referred to as the 'like-minded' in this context – calling for a new round of the GGE. The second was submitted by Russia and supported by China, calling for an Open-Ended Working Group (OEWG) to discuss roughly the same issues. Both were voted through by the General Assembly in substantial and significantly overlapping numbers and the twin processes have started in 2019.

These diplomatic processes surrounding cyber norms and their voluntary, non-binding nature exemplify the different outlooks of China and Russia on the world order and their place and role in it. China and Russia want to partake in creating norms for responsible behavior in cyberspace. Yet, their rationale for it differs. China has not voiced substantive disagreement with the norms and format of the GGE. Most norms developed by now are, in principle, acceptable to them. The point of contestation lies with those who develop, implement, and interpret them. Non-binding, voluntary norms aimed at shaping State behaviour in their use of ICT have been and are still perceived to be a largely US-led project developed as an alternative to Chinese and Russian proposals of binding normative solutions. China, as a global power, will only feel bound by an international framework that it has helped shape, that binds the US in equal measure. Russia, on the other hand, takes a conservative stance when it comes to norms. To Russia, norms are viewed as binding. Deriving from the positivistic legal culture, non-binding norms are merely an intermediary step toward binding norms. Russia perceives itself as a defender of the international order that needs to counter-balance the interpretative right of the West.

[46] On the UN GGE process, see: United Nations Office for Disarmament Affairs (UNODA). (2019) "Fact sheet: Developments in the field of information and telecommunications in the context of international security". UNODA, July 2019. For a broader view on the cyber norms process, see: Martha Finnemore & Duncan B. Hollis. (2016). "Constructing Norms for Global Cybersecurity". *The American Journal of International Law,* 110 (3): pp. 425-479.

[47] United Nations General Assembly. (2010). "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General", UN Document A/65/201, 30 July 2010; United Nations General Assembly. (2013). "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General", UN Document A/68/98, 24 June 2013; United Nations General Assembly. (2015). "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General", UN Document A/70/174, 22 July 2015.

[48] See, for example: Alex Grigsby. (2017). "The End of Cyber Norms". *Survival,* 59 (6), pp. 109-122.

Thus, Russia is willing to entertain the idea of non-binding and voluntary norms solely because it bears the promise of a binding future normative framework. While China is willing to wait to counter Western normative imperialism, Russia is perhaps more eager to get a result in the next iteration of the UN GGE and the newly created OEWG, especially given its long-term sponsorship of the former and its proposal of the latter.

Russia has framed the 2018 resolution[49] calling for the establishment of an OEWG as a great success. The Russian narrative of the process sees the OEWG as a platform to discuss the new cyber order that would move away from governance by elite clubs and bring “democratization” (i.e. greater participation from smaller and non-Western countries) to the process. However, given Chinese and Russian ideas of great power politics and sovereignty, the extent to which they actually desire that greater participation is doubtful, particularly if those countries are skeptical of the Chinese or Russian position. It does, nonetheless, put Russia in a position to exert global leadership. One of the major lines of contention in both the UN GGE and OEWG will be the issue of sovereignty that both China and Russia regard as a fundamental norm. China has generally been skeptical on intervention, particularly where justified on the basis of norms such as human rights and the responsibility to protect (R2P). Moreover, in both Russia and China the right to self-determination goes hand in hand with a policy of building capacity to make sure any intervention by outsiders can be blocked, as evidenced by attempts to control the national information sphere through the Great Firewall of China or the recent legislation on RusNET. Given the strong link between (cyber) sovereignty and the protection of the national information sphere, sovereignty, as well as its boundaries in cyberspace, will be contentious. This contestation is exacerbated by the diverging views over the status of sovereignty in international law among the likeminded. The British approach[50] of seeing sovereignty as a mere general principle of international law, instead of a steadfast rule, problematizes not only the general principle that international law applies online as it does offline, but also all of the principles and rules that derive from the rule of sovereignty.[51] Here, the likeminded need to take steps in clarifying how they understand the international law applies in cyberspace and avoid cherry-picking from the body of international law in order to substantiate their case to prevent the creation of *lex specialis* in cyberspace.

Geopolitical and military relations

In military terms the two countries differ widely. Unlike the US and Russia, China does not have a battle-hardened military but is investing heavily in the growth of its military. Chinese military doctrine has taken a high-tech turn in recent years, highlighting the need for capabilities to attack Command and Control structures in and through cyberspace as well as space.[52] The investment

[49] United Nations General Assembly. (1998). “Letter dated 98/09/23 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General”. UN Document A/C.1/53/3, 23 September 1998.

[50] Jeremy Wright. (2018). “Cyber and International Law in the 21st Century”. Speech from the UK’s Attorney General’s Office, 23 May 2018.

[51] Cf. French Ministry of Defence. (2019). *Droit International Appliqué aux Opérations dans le Cyberespace,* 4 October 2019; Kaljulaid, Kersti. (2019). “President of Estonia: international law applies also in cyber space”. Speech at CyCyon 2019, 29 May 2019.

[52] Elsa B. Kania & John K. Costello. (2018). “The Strategic Support Force and the Future of Chinese Information Operations”. *The Cyber Defense Review,* 3 (1): pp. 105-122.

in a high-tech military also makes them more vulnerable to attack via digital means. Some experts highlighted the disconnect between Chinese military doctrine, heavily focused on cyber warfare, and the actual practice which focuses on cyber defense, digital control over the national information sphere and (economic) cyber espionage. However, as Chinese military power grows and geopolitical tensions rise, doctrine will be taken more seriously by adversaries in the future. Russia's military cyber presence is more focused on information warfare and fits in a more general Russian trend of favoring conflicts in which plausible and implausible deniability creates room to maneuver.[53] Though a nuclear power and a weapons developer at the moment, Russia lacks the operational military means to project power globally – in spite of having a decisive role in nearby theatres of war such as Syria. Cyber operations however, are an ideal strategy for a global reach. One of the experts characterized cyber operations as "the new nuclear" for Russia, in the sense of being in the game as a top tier power. In terms of future stability in cyberspace, and beyond, the interaction effects between the doctrinal shifts in China, Russia and the US will be crucial. All three countries are upping their game in terms of cyber military and intelligence operations with increasingly invasive operational concepts and strategies. Escalation of cyber conflict is more likely to arise between the US and Russia, due to their tumultuous relationship, and this may affect the Sino-Russian relationship. China is unlikely to back any escalation with the US that is imposed on it by erratic Russian behavior. The bandwidth between ignoring it and actively distancing oneself from an ally is, however, still wide.

Conclusions

While China and Russia clearly share important elements of their worldview, as well as particular terms and concepts, the similarity between them should not be overstated. Both countries have a markedly different geopolitical outlook and interests in cyberspace. This means China is more invested in the long-term stability of the global cyber system than Russia is.

Russia's role in cyberspace is characterised by both an early diplomatic engagement with the issue of international peace and stability in cyberspace and as the suspected originator of disruptive and (potentially) destabilising cyber operations. Engagement with Russia on both is necessary but it requires careful consideration to pick the topics on which actual progress is possible. China's rise in cyberspace, as in other policy areas, creates not only political challenges, but also intellectual ones. China, as a cyber-power, is here to stay, making engagement the only plausible option. In many areas, including cybersecurity and technical standards, it is an inevitable counterpart, even though in other areas, it will remain a competitor or even an opponent. The task will be to not only identify areas for collaboration, but also identify potentially counterproductive Western policies that exacerbate distrust. China will only comply with rules it sees other major powers, particularly the US, complying with.

[53] Rory Cormac & Richard J. Aldrich. (2018). "Grey is the new black: covert action and implausible deniability". *International Affairs*, 94 (3): pp. 477–494.

Policy take-aways

- Given the political investment of especially Russia in the OEWG, this process is joined at the hip with the UN GGE. This is a moment of Mutually Assured Diplomacy: either both processes yield a result or neither will.
- It would be unwise to view cyber questions merely in isolation, as they are inextricably linked to the more general fissures emerging in geopolitics, which manifest themselves across the economic and political realms.
- The likeminded need a solid narrative to back up their 'no' to a special cyber treaty. It is vital that more countries put to paper how they see the application of international law in cyberspace, as some states have already been doing (United Kingdom, Estonia, Australia, France).
- A functional breakdown of the rules-based order could be helpful to see where engagement is more and less possible. For instance, it might be easier to cooperate in areas that are more technological, such as inter-CERT cooperation, while avoiding more politically sensitive areas, such as law enforcement cooperation and online rights.
- A (re)engagement with China and Russia through track 1.5 and 2.0 dialogues (perhaps along different aspects of the liberal order) could identify issues for cooperation and methods to do so.
- There is a need to analyse and prepare for Russian and Chinese reactions to (a) a US military doctrinal shift (more aggression in cyber) and (b) the EU cyber sanctions regime in policy development.

Authors

Dennis Broeders is Associate Professor of Security and Technology and Senior Fellow of The Hague Program for Cyber Norms at the Institute of Security and Global Affairs at Leiden University. Prior to joining Leiden University, he was a Senior Research Fellow at the Netherlands Scientific Council for Government Policy and Professor of Technology and Society at Erasmus University Rotterdam.

Liisi Adamson is a PhD researcher at the Hague Program for Cyber Norms. Prior to commencing her PhD studies Liisi served as a research fellow at the Cyber Policy Institute in Estonia (2014-2017) and as an advisor to the Estonian delegation to the UN Group of Governmental Experts on Information Security (2016-2017).

Rogier Creemers is an Assistant Professor in the Law and Governance of China at Leiden University, and an Associate Fellow of The Hague Program for Cyber Norms at the Institute of Security and Global Affairs. His research investigates China's domestic technology policies, as well as China's participation in global cyber affairs. His work has been published, amongst others, in The China Journal and the Journal of Contemporary China. He is also a founding member of DigiChina, a project run in cooperation with New America, as well as a frequent contributor to international news media.

Acknowledgements

The authors would like to thank the participants in the workshop 'China and Russia in global Cyberspace', held in May 2019 in the Hague, for their time and participation and for their contribution to the ideas and insights gathered in this policy brief. They would also like thank Bobo Lo and Camino Kavanagh for their insightful comments on an earlier draft. Lastly, they would like to thank Corianne Oosterbaan for the smooth organisation of the workshop and her editorial assistance.

All of the activities and publications of The Hague Program for Cyber Norms are supported by a grant of the Dutch Ministry of Foreign Affairs.

Contact information

E-mail: info@thehaguecybernorms.nl
Website: https://www.thehaguecybernorms.nl
@HagueCyberNorms

Address
The Hague Program for Cyber Norms
Faculty of Governance and Global Affairs
Leiden University
Hague Campus
Turfmarkt 99
2511 DP The Hague

Colofon
Published October 2019.

Graphic design: www.pauloram.nl

THE HAGUE
PROGRAM
for Cyber Norms

LEIDEN
ASIA
CENTRE

Universiteit
Leiden