The Kremlin Leverages Cyber Cooperation Deals

By Zachary Greenhouse with George Barros

KT: *The Kremlin is successfully expanding its global cyber footprint to contest the West by signing cooperation deals in the field of international information and communications technologies (ICTs). The Kremlin prioritizes these deals to set conditions to expand its access to global technical networks and infrastructure, as well as to develop its human networks and institutional links around the world. The Kremlin launched this campaign in 2014, shortly before releasing an updated information security doctrine in 2016, which continues to guide Russian cyber policy.[1] This campaign supports the Kremlin's strategic goal of subverting Western global influence via nontraditional means. The Kremlin will likely use these deals to increase its cyber-attack capabilities and expand influence in key regions. The Kremlin may additionally use these deals to garner support for a Kremlin-friendly resolution on ICTs in the UN to shape international norms in cyberspace.*

This piece supports a forthcoming report from ISW on Putin's geopolitical adaptations since 2014.

The Kremlin is adapting its expanding cyber capabilities and influence by leveraging international information and communications technologies (ICT) cooperation agreements. The Kremlin signed over 30 ICT deals bilaterally and with multinational regional organizations since 2014. This campaign supports a stated objective of Russia's 2016 information security doctrine to prioritize expanding Russia's international cyber cooperation.[2] The Kremlin continues to prioritize this effort as of August 2020. The Kremlin uses these deals to set conditions for Russia to expand its human and institutional networks in the cybersecurity sphere, export its image abroad as a trustworthy partner in cyberspace, reinforce Kremlin narratives around the world, and expand its access to global cyber infrastructure.

The Kremlin's expanding ICT partnerships advance multiple objectives:

The Kremlin is using these deals to reinforce Kremlin narratives around the world and posture as an alternative to Western ideas in cyberspace. The Kremlin's cyber deals advance its effort to facilitate resistance to "Western digital neocolonialism," a term Russian Security Council Secretary Nikolai Patrushev coined in 2019.[3] The Kremlin fears an expansion of Western ideas throughout the global information space, particularly to regions in which the Kremlin historically has had influence.[4] The Kremlin intends to counter the expansion of Western ideas in the information space and cement its existing relationships with countries that it considers vulnerable to Western influence. Kremlin deals may disrupt or discourage Western cooperation with countries that Russia engages with actively, advancing the Kremlin's goal of creating alternative international structures.

The Kremlin is expanding its human network and institutional links in the professional cybersecurity landscape. The Kremlin's new ICT deals stipulate cooperation in specific technical areas. The Kremlin's deals with China, India, Belarus, the Philippines, South Africa, and Cuba, for example, stipulate cooperation in joint cyber defense exercises, fighting cybercrime, and wargaming in the cyber domain.[5] Many of the Kremlin's new ICT deals have limited substance but serve as calls to action for greater cooperation. Even simple ICT agreements grant the Kremlin opportunities to participate in cybersecurity discussions, cultivate human relationships with foreign cybersecurity professionals, and develop potential avenues for deeper cooperation. The Kremlin's deals with regional and international organizations indicate the Kremlin is prioritizing maximizing the reach and scope of its individual deals. The Kremlin has previously used a similar "foot in the door" approach with media and security cooperation deals.[6]

The Kremlin seeks to contest the West in cyberspace by leveraging international organizations. The Kremlin's information security policy, which was updated in 2016, calls for an independent Russian information policy and the elimination of Russian dependency on foreign ICTs.[7] The Kremlin aims to pull as many countries into its orbit as possible to expand its soft power capabilities in cyberspace. Many of

the Kremlin's ICT deals stipulate cooperation in international institutions, particularly prioritizing the United Nations as a discussion forum to leverage Russia's veto power and influence within that body.[8] Russia has been a key voice in two ongoing UN processes to update the 2004 resolution on ICT use.[9] The Kremlin hopes to skew the UN discussions on ICT use toward combatting illegal online content, rather than ensuring information infrastructure security.[10]

The Kremlin is setting conditions to expand its access to more countries' cyber systems. Several of the Kremlin's ICT deals indicate the Kremlin seeks to expand Russian access to cyber infrastructure and systems.[11] Several deals stipulate Russian companies providing cybersecurity services to governments.[12] For example, The MePHI Institute, a Russian state-owned nuclear research institute, signed a deal to provide cybersecurity services for a Brazilian company that controls much of Brazil's water and sanitation infrastructure.[13] The access these deals provide may enhance the Kremlin's cyberattack capabilities. The Kremlin has displayed its capability to exploit backdoors in compromised networks to perform cyberattacks and hacks against multiple countries, including Germany, Estonia, Ukraine, and Georgia, since 2007.[14]

Forecast: The Kremlin will prioritize cyberspace as a domain in which to contest the West at low-cost in the future. The Kremlin will continue to pursue bilateral and multilateral cyber deals to further the objectives outlined above. The Kremlin will likely increasingly focus on Southeast Asia and South/Central America as priority regions, as these areas are rapidly growing in the ICT sector, and cooperation in these areas provides other strategic advantages for the Kremlin, as seen in ISW assessments on Kremlin security and media cooperation deals in the same timeframe.[15] The Kremlin will use these deals to increase its capability to perform cyberattacks. The Kremlin's cyber cooperation deals additionally set conditions to support future Russian hybrid war campaigns by increasing the Kremlin's ability to create and maintain malign information campaigns and disrupt its opponents in cyberspace.[16] The Kremlin may also pressure other nations into supporting Russia's UN resolution on ICT use to shape global norms to its own advantage.

Recommendation: The West should monitor the Kremlin's efforts to increase its international access and profile in cyberspace and act to counter Russian expansion in cyberspace. The West should contest the Kremlin's assertion that Russia is a trusted actor in cyberspace by drawing attention to the Kremlin's malign cyber activities. The Kremlin's resistance to "Western digital neocolonialism" seeks to increase centralization and control over cyberspace, not the free alternative the Kremlin attempts to frame these efforts as supporting. While it might be tempting to respond aggressively with cyberattacks or a concentrated pressure campaign in support of Western values, the West should instead rely on promoting its principles of freedom and fairness to combat Russian expansion in the information space.

---

[1] ["On the Approval of the Doctrine of Information Security of the Russian Federation,"] *Kremlin,* December 5, 2016, http://kremlin(.)ru/acts/bank/41460/page/2.
[2] ["On the Approval of the Doctrine of Information Security of the Russian Federation,"] *Kremlin,* December 5, 2016, http://kremlin(.)ru/acts/bank/41460/page/2.
[3] ["Nikolai Patrushev: Security in the Modern World,"] *Rossiyskaya Gazeta,* November 11, 2019, https://rg(.)ru/2019/11/11/patrushev-ssha-stremiatsia-izbavitsia-ot-mezhdunarodno-pravovyh-ramok.html.
[4] For example, the number of deals in southeast Asia indicates that this region remains a Kremlin priority area. ISW previously assessed that the Kremlin is using Singapore, a US ally, as a nexus for expanding influence in southeast Asia in October 2019:
George Barros and Nataliya Bugayova, "The Kremlin's Outreach to Singapore," *Institute for the Study of War,* October 18, 2019, http://iswresearch.blogspot.com/2019/10/russia-in-review-kremlins-outreach-to.html;
"Russian security chief discusses cooperation with Interpol, cybersecurity in Singapore," *TASS,* August 29, 2019, https://tass(.)com/society/1075608.

[5] **Philippines:** "DICT, Russian company to cooperate on Cybersecurity initiatives," *Philippines Department of Information and Communications Technology*, September 25, 2018, https://dict.gov(.)ph/dict-russian-company-to-cooperate-on-cybersecurity-initiatives;
Belarus: "Belarus, Russia to expand cooperation in information security," *Belta,* September 10, 2019, https://eng.belta(.)by/politics/view/belarus-russia-to-expand-cooperation-in-information-security-124031-2019/;
South Africa: "Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security," *Russian MFA,* September 4, 2017, https://www.mid(.)ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2854430;
Cuba: ["Agreement between the Government of the Russian Federation and the Government of the Republic of Cuba on cooperation in providing international information security,"] *Russian MFA,* January 2, 2015, https://www.mid(.)ru/ru/foreign_policy/international_contracts/2_contract/-/storage-viewer/bilateral/page-2/44171?_storageviewer_WAR_storageviewerportlet_advancedSearch=false&_storageviewer_WAR_storageviewerportlet_keywords=%D0%9A%D1%83%D0%B1%D0%B0&_storageviewer_WAR_storageviewerportlet_fromPage=search&_storageviewer_WAR_storageviewerportlet_andOperator=1.

[6] Nataliya Bugayova and George Barros, "The Kremlin's Expanding Media Conglomerate," *Institute for the Study of War,* January 15, 2020, https://www.iswresearch.org/2020/01/the-kremlins-expanding-media.html; Nataliya Bugayova, et al., "Russia in Review: Russian Security Cooperation Agreements Post-2014," *Institute for the Study of War,* May 15, 2020, https://www.iswresearch.org/2020/05/russia-in-review-russian-security.html.

[7] ["On the Approval of the Doctrine of Information Security of the Russian Federation,"] *Kremlin,* December 5, 2016, http://kremlin(.)ru/acts/bank/41460/page/2.

[8] The UN resolution on ICT use is a critical development, as actions in cyberspace have not yet been codified in international law. Earlier conversations in the UN in 2013 and 2014 failed due disagreements between Russia and the West regarding the resolution's main focus. The Kremlin wanted the resolution to focus on internet content, while Western states wanted it to focus on protection of information infrastructure. The Kremlin's desire to focus a UN resolution on online content would further legitimize their legal basis for internet censorship and control.

[9] "Developments in the field of information and telecommunications in the context of international security," *United Nations*, https://www.un.org/disarmament/ict-security/. Russia introduced the initial draft resolution into the UNGA, which was passed without a vote in 2004.
[10] "Fact Sheet: Developments in the Field of Information and Communications Technologies in the context of International Security," *United Nations,* https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.
[11] **Brazil:** Luiz Padilha, ["Brazil buys Russian innovation to protect companies from cyber attacks,"] *["Air and Sea Defense,"]* July 20, 2017, http://www.defesaaereanaval(.)com.br/brasil-compra-inovacao-russa-para-protecao-de-empresas-contra-ataques-ciberneticos/.
Kazakhstan: Anna Gussarova, "Kazakhstan Launches 'Cyber Shield' Concept," *Jamestown Foundation,* November 20, 2017, https://jamestown.org/program/kazakhstan-launches-cyber-shield-concept/; Nikolai Enelane, ["Why the state is willing to pay for information security,"] *InformBuro,* June 19, 2017, https://informburo(.)kz/stati/pochemu-gosudarstvo-gotovo-platit-za-nashu-i-svoyu-cifrovuyu-bezopasnost-.html; ["Kazakhtelecom and Solar Security signed a memorandum of partnership and interaction in the field of cybersecurity,"] *Rostelekom-Solar,* April 27, 2017, https://rt-solar(.)ru/events/news/906/;
Vietnam; ["Russian company will help Vietnam create antivirus for government agencies,"] *Russian Ministry of Digital Development, Communications and Mass Media,* August 7, 2019, https://digital.gov(.)ru/ru/events/39250/;

North Korea; "Russian firm provides new internet connection to North Korea," *Reuters,* October 2, 2017, https://www.reuters.com/article/us-nkorea-internet/russian-firm-provides-new-internet-connection-to-north-korea-idUSKCN1C70D2; Martyn Williams, "Russia Provides New Internet Connection to North Korea," *38 North,* October 1, 2017, https://www.38north.org/2017/10/mwilliams100117/.

[12] **Vietnam**; ["Russian company will help Vietnam create antivirus for government agencies,"] *Russian Ministry of Digital Development, Communications and Mass Media,* August 7, 2019, https://digital.gov(.)ru/ru/events/39250/;

North Korea; "Russian firm provides new internet connection to North Korea," *Reuters,* October 2, 2017, https://www.reuters.com/article/us-nkorea-internet/russian-firm-provides-new-internet-connection-to-north-korea-idUSKCN1C70D2; Martyn Williams, "Russia Provides New Internet Connection to North Korea," *38 North,* October 1, 2017, https://www.38north.org/2017/10/mwilliams100117/.

[13] Luiz Padilha, ["Brazil buys Russian innovation to protect companies from cyber attacks,"] *["Air and Sea Defense,"]* July 20, 2017, http://www.defesaaereanaval(.)com.br/brasil-compra-inovacao-russa-para-protecao-de-empresas-contra-ataques-ciberneticos/.

[14] **Estonia**: Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired,* August 21, 2007, https://www.wired.com/2007/08/ff-estonia/;

Georgia: Sarah P. White, "Understanding Cyber Warfare: Lessons from the Russia-Georgia War," *Modern War Institute at West Point,* March 20, 2018, https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf;

Ukraine: Donghui Park, et al, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," *JSIS at the University of Washington,* October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#_ftn2;

Germany: Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections," *Brookings,* June 28, 2017, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[15] **Media:** Nataliya Bugayova and George Barros, "The Kremlin's Expanding Media Conglomerate," *Institute for the Study of War,* January 15, 2020, https://www.iswresearch.org/2020/01/the-kremlins-expanding-media.html; **Security:** Nataliya Bugayova, et al., "Russia in Review: Russian Security Cooperation Agreements Post-2014," *Institute for the Study of War,* May 15, 2020, https://www.iswresearch.org/2020/05/russia-in-review-russian-security.html.

[16] ISW's upcoming report on Russian Hybrid War explores this topic in greater detail.