Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Sean S. Costigan, *Connections QJ* 20, no. 2 (2021): 9-13
https://doi.org/10.11610/Connections.20.2.01

Research Article

Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty

Sean S. Costigan

George C. Marshall European Center for Security Studies, https://www.marshallcenter.org/

Abstract: Under the guise of combating cybercrime, two radically different visions of cyberspace compete for attention on the international stage: a free-flowing model of cyberspace that democracies have championed is now challenged by a so-called sovereign model. Counter-democratic initiatives to reframe cyberspace in strictly national terms are underway with the likely result of decreased cooperation and increased risks of conflict and cybercrime.

Keywords: Cybercrime, Cyberspace, Sovereignty, Cooperation, Conflict

Global unrest is fast becoming the norm in cyberspace, where cybercriminals operate with relative impunity, and novel technologies allow nation-states to sharpen their practice of influence operations. There is a near-constant rate of hacks against computers – by one recent count every 39 seconds on average for devices connected to the Internet.[1] If cybercrime is not tackled, at risk is nothing less than trust in the government's ability to deliver on the promise of security. 61% of Europeans worry that elections can be manipulated through cyberattacks. One in three Americans will find themselves a victim of some form of cybercrime this year alone, not to mention the risks of state interference.

Disinformation has consumed many news and policy cycles, no less now in the time of COVID-19. Russian disinformation campaigns have regularly pushed

[1] "Hackers Attack Every 39 Seconds," *Security Magazine*, February 10, 2017, https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.

out propaganda about the virus through think-tanks and suspect news services.[2] Cyberspace has emerged as a national security complex, affecting as it does governments, corporations, and individuals alike. Given this state of affairs, a universal cybercrime treaty would seem to benefit all.

Under the guise of combating cybercrime, two radically different visions of cyberspace compete for attention on the international stage. The first may be broadly characterized as a free-flowing model of cyberspace and has been championed by democracies. It is challenged by the second, the so-called "sovereign model," where the primary focus is state control over information and, ultimately, people.

On 18 November 2019, a United Nations committee passed a Russia-backed cybercrime resolution by a vote of 88 to 58, with 34 countries abstaining. Russia's successful vote set up an "Open-Ended Working Group" to examine cybercrime and methods to prevent it. While this development might sound potentially beneficial, it has direct consequences for the Budapest Convention on Cybercrime[3] and existing mechanisms for improving the fight against cybercrime, international and national legal efforts, as well as long-term foreign policy impacts in many areas beyond cyberspace.

The Budapest Convention is the only convention on cybercrime. However, it has come under sustained pressure from Russia and its foreign policy partners that argue its very existence is an effort to violate sovereignty. (Note that the Budapest Convention is open to the accession of countries that are not parties to the Council of Europe and is the means for international cooperation to tackle cybercrime.)

Russia has also been actively trying to physically move current discussions on cybercrime from their home in Vienna, Austria (where decisions are made through consensus) to New York, where a majority vote would seem to give Russia and China a significant advantage in the future proceedings.[4]

Moreover, Russia and China may parlay such wins at the United Nations to further not just their overarching goals of challenging the existence of universal human rights and the ideals of an open, free, and indivisible Internet, but also the post-World War II world order, which Russia currently, and China more principally, regards to primarily be a Western construction – and thus, in their conception, unjustly benefitting Western states.

[2] Julian E. Barnes and David E. Sanger, "Russian Intelligence Agencies Push Disinformation on Pandemic," *The New York Times*, July 28, 2020, https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html.

[3] Council of Europe, "Convention on Cybercrime," Treaty No. 185, Budapest, November 23, 2001, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[4] U.S. Department of State, "State Department Official on Multilateral Cyber Efforts," Special Briefing, Office of the Spokesperson, Press Correspondents Room, December 19, 2019, https://web.archive.org/web/20191220024014/https://www.state.gov/state-department-official-on-multilateral-cyber-efforts/.

Considering these moves, this article argues that the West should prepare for future international negotiations that might not go according to plan, to include further gains by China and Russia to seek control over information and alter the course of cyberspace as we know it.

The Russian proposal for a global cybercrime convention as well as Russia's eagerness to further the "Open-ended Working Group on Developments in the Field of information and telecommunications in the context of international security"[5] are primarily political moves to strengthen the Russian goal of establishing "the system of international information security."[6] The system the Kremlin seeks to achieve would be based on a "Convention on International Information Security," with the United Nations and the International Telecommunications Union assigned to play major roles. Moreover, this Russian conception leans on strong, even absolute, state sovereignty, which undermines and overrides international obligations the state may have or be interpreted to have.[7]

Russian arguments for the purposes of a so-called sovereign internet (known as *RuNet*) stress several aspects of security by autonomy. The objective of a separate Russian internet was outlined in the 2017 information security doctrine[8] as "developing a national system of the Russian Internet segment management." The context of this ambition being "of ensuring information security in the field of strategic stability and equal strategic partnership" implicitly but effectively refers to the perceived information security threat from the United States. The purpose of the "national segment of the Internet," as it is also called, was to protect information as such and secure Russian critical infrastructure in the event of threats to the stability, security, and functional integrity.

Some Russians have come to justify the ostensible need to maintain Russian-to-Russian traffic within territorial borders through the use of financial arguments: by this reckoning, the cost of international routing may, in the future,

[5] United Nations Office for Disarmaments Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security," https://www.un.org/disarmament/ict-security/.

[6] "Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020," approved by the President of the Russian Federation on 24 July, 2013, accessed September 29, 2020, http://en.ambruslu.com/highlights-in-russia/basic-principles-for-state-policy-of-the-russianfederation-in-the-field-of-international-information-security-to-2020.html.

[7] Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law': Tightening Control and Accelerating the Splinternet," *German Council on Foreign Relations*, January 16, 2020, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

[8] *Doctrine of Information Security of the Russian Federation*, Approved by Decree of the President of the Russian Federation No. 646, December 5, 2016.

become too expensive.[9] The demand to pre-install Russian software to "track, filter, and reroute internet traffic"[10] can be read in the contexts of information security, critical infrastructure protection, and boosting national research and development markets.[11] Obviously, widening the coverage of federal (Roskomnadzor's) enforcement mechanisms from routing traffic to all ITC devices also increases political and informational control over individuals.

It would appear then that these moves are intended to create a cloud of uncertainty that would undermine work done in the past and consensus regarding international norms in cyberspace while subverting the core values of an open, free and accessible Internet. Russia and China are working hand-in-hand to enforce what many experts maintain is a dystopian, state-control view of cyberspace on the world. This means exercising their authoritarian policies that are in stark contradiction with the democratic order and undercutting the framework of global economic order and business interests over the long term.

While the voting in the UN 3rd committee showed that there is no consensus to start negotiation or to establish a new legal instrument on cybercrime, it should be clear that this effort will not go away on its own. Furthermore, there is no consensus on the legal scope that such a new treaty on this issue should have. In addition, Western European nations appear to recognize that such a process would serve to divert efforts from national legislative reforms and current capacity building, essentially throwing a wrench into these efforts.

A new international legal instrument on cybercrime would duplicate existing work and preempt the conclusions of the open-ended intergovernmental UN expert group (IEG)[12] to conduct a comprehensive study of the problem of cybercrime and responses to it by member states.

Russia has not just maintained but has also developed and strengthened its call for an "international information security system." Meanwhile, some experts argue that the West has not been particularly successful in its efforts to convince and engage states outside its perimeter.[13] Moscow and Beijing appear largely immune to name-and-shame strategies or accusations of cyberattacks and

[9] According to discussions with Kaspersky experts, currently only 2% of Russian-to-Russian traffic crosses its national borders.

[10] "Russia Internet: Law Introducing New Controls Comes into Force," *BBC*, November 1, 2019, https://www.bbc.com/news/world-europe-50259597.

[11] For an opposite view see Alexandra Prokopenko, "Russia's Sovereign Internet Law Will Destroy Innovation," *The Moscow Times*, April 21, 2019, www.themoscowtimes.com/2019/04/21/russias-sovereign-internet-law-will-destroy-innovation-a65317.

[12] The IEG is the main process at the level of the United Nations on the issue of cybercrime.

[13] Sally Adee, "The Global Internet Is Disintegrating: What Comes Next?" *BBC*, May 15, 2019, www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

espionage, such as with the SolarWinds breach.[14] Meanwhile, the authority of like-minded Western countries has been affected by leaks of foreign espionage,[15] news reports of mass surveillance,[16] weakening encryption,[17] and especially of government expectations of corporate assistance. To effectively push back on counter-democratic initiatives, the West needs to undermine one of the three pillars in the Kremlin's strategy: the general distrust towards ICTs, the insufficiency of existing international law, or the existential threat narrative. Another way to increase resilience in cyber discourse is to identify shared national interests and objectives across camps and continents, such as through the Framework for Responsible State Behavior in Cyberspace[18] and the Paris Call for Trust and Security in Cyberspace.[19] To advance, the West needs to prepare for treaty negotiations as one possible future. Preparing for that worst-case scenario, it should be possible to find new openings to avoid it.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Sean S. Costigan – see the CV on page 8 of this issue, https://doi.org/10.11610/Connections.20.2.00

[14] Sean S. Costigan, "Charting a New Path for Cybersecurity after SolarWinds." *Diplomatic Courier*, January 4, 2021, www.diplomaticourier.com/posts/charting-a-new-path-for-cybersecurity-after-solarwinds.

[15] Patricia L. Bellia, "WikiLeaks and the Institutional Framework for National Security Disclosures," *Yale Law Journal* 121, no. 1448 (2012), April 2, 2012, Notre Dame Legal Studies Paper No. 12-59, https://ssrn.com/abstract=2033207.

[16] Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (June 2014): 121-144.

[17] Aaron Brantly, "Banning Encryption to Stop Terrorists: A Worse than Futile Exercise," *CTC Sentinel* 10, no. 7 (August 2017): 29-33, https://ctc.usma.edu/wp-content/uploads/2017/08/CTC-Sentinel_Vol10Iss7-10.pdf.

[18] "Joint Statement on Advancing Responsible State Behavior in Cyberspace," United States Department of State, September 23, 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/ and "Eleven Norms of Responsible State Behaviour in Cyberspace," Federal Department of Foreign Affairs FDFA, April 7, 2021, https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html.

[19] "Paris Call for Trust and Security in Cyberspace – Paris Call," https://pariscall.international/en/.

Acknowledgment

Connections: The Quarterly Journal, Vol. 20, 2021, is supported by the United States government.