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

Sean S. Costigan, *Connections QJ* 22, no. 1 (2023): 91-98
https://doi.org/10.11610/Connections.22.1.07

Research Article

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

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.

The digital frontier, celebrated by many since its inception as a bastion of free speech and worldwide connectivity, is now at a major crossroads between two widely divergent perspectives that will impact the future of cyberspace and future prosperity. The first, which may be described as the open cyberspace model championed by idealists and democracies, is increasingly in confrontation with a restrictive "sovereign" internet paradigm, favored by authoritarian governments. As the debates about the future of cyberspace play out, the gap between these views is being exploited by cybercriminals whose exploits—and the damage they cause—have now been widely recognized in national security strategies worldwide.

The flow of information—the lifeblood of our modern global systems—is imperiled. Governments and national critical infrastructures are coming under in-

Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

creasing cyber attacks; doubling by one account and with no end in sight.[1] Increasingly, cyberspace is being seen as a ferment for global malaise, as cybercriminals exploit vulnerabilities with little fear of repercussions and states hide behind attribution challenges despite technical attribution becoming more available and widely promoted.[2] With hacks occurring almost every 39 seconds for internet-connected devices, the scale of the threat is undeniable. The stakes are high; if cybercrime is not addressed, public faith in governmental security assurances may further erode, and economies may be damaged. Public anxiety is evident with, for example, more Europeans concerned about attacks against national governments.[3] Furthermore, an estimated one-third of Americans will face some cybercrime this year, highlighting the urgent need to tackle both criminal and state-sponsored digital threats.

Public trust in national governments and international systems is challenged on multiple fronts. By the OECD's measure, as of 2022, there is an even split between those who trust government and those who do not, with younger people having even lower levels of trust.[4] An entry on the International Monetary Fund's public website aptly describes the lack of trust in the global order, with particular attention paid to four factors: the reaction to globalization, financial crises, technology and AI, and the rise of populism.[5] In this light, Russian disinformation campaigns accelerated during the COVID-19 pandemic, serving to destabilize trust further,[6] and China stands accused of further amplifying the chaos as it continues a wholesale theft of state secrets and intellectual property as well as disinformation campaigns.

Moscow and Beijing appear largely immune to name-and-shame strategies or accusations of cyberattacks and espionage, such as with the SolarWinds

[1] Jonathan Reed, "High-impact Attacks on Critical Infrastructure Climb 140 %," *Security Intelligence*, June 26, 2023, https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/.

[2] Jake Sepich, "The Evolution of Cyber Attribution," *American University*, April 19, 2023, https://www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm.

[3] Thomas Macaulay, "Spate of Cyber Attacks in Europe Increases Concerns about Government Defenses: The Public Sector Is a Growing Target for Cybercrime," *TNW*, November 9, 2022, https://thenextweb.com/news/cyber-attacks-european-governments-increase-concerns-public-sector-defenses.

[4] OECD, "Trust in Government," https://www.oecd.org/governance/trust-in-government/.

[5] David Lipton, "Trust and the Future of Multilateralism," *IMF*, May 10, 2018, https://www.imf.org/en/Blogs/Articles/2018/05/10/blog-trust-and-the-future-of-multilateralism.

[6] "Disinformation and Russia's War of Aggression against Ukraine: Threats and Governance Responses," *OECD*, November 3, 2022, https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/.

breach, which the United States formally attributed to Russia.[7] Meanwhile, the authority of like-minded Western countries has been affected by leaks of foreign espionage,[8] news reports of mass surveillance,[9] weakening encryption,[10] and general opacity on a wide range of emerging technological and policy challenges from facial recognition to artificial intelligence.

A Vision of the Future, Grounded in the Present

Since at least 2016, Russian disinformation efforts have been a subject of deep concern for many governments and researchers around the world. These campaigns of political warfare, sometimes referred to in the security community by the phrase "active measures," have been employed by Russia for decades.[11] But with the advent of social media and the internet, their costs have shrunk while their reach and potential impact have been vastly amplified. In the era of COVID-19, disinformation has taken center stage in numerous news and policy discussions. Notably, Russian-driven disinformation efforts have consistently promoted misleading narratives about the virus via suspect news platforms and supposed think tanks.[12]

Into this dynamic mix comes the work of cyber saboteurs of many stripes, from hacktivists to those in the service of intelligence agencies. Recently, NATO itself has become the target of political hacks, with damaging leaks of internal documents.[13] Manipulating the narrative through theft and leaking of select information or targeting vocal minorities for exploitation has become a new norm.

[7] 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.

[8] 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.

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

[10] 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.

[11] Jolanta Darczewska and Piotr Żochowski, *Active Measures. Russia's Key Export*, Point of View 64 (Warsaw, Poland: OSW Centre for Eastern Studies, June 2017), https://www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export.

[12] Ben Dubow, Edward Lucas, and Jake Morris, *Jabbed in the Back: Mapping Russian and Chinese Information Operations During the COVID-19 Pandemic* (Washington D.C.: Center for European Policy Analysis (CEPA), December 2, 2021), https://cepa.org/comprehensive-reports/jabbed-in-the-back-mapping-russian-and-chinese-information-operations-during-the-covid-19-pandemic/.

[13] A.J. Vicens, "NATO Investigating Breach, Leak of Internal Documents," *CyberScoop*, October 3, 2023, accessed October 5, 2023, https://cyberscoop.com/nato-siegedsec-breac/.

In turn, democratic governments have categorized the variety of information campaigns visible today by using the rubric MDM, for misinformation, disinformation, and malinformation.[14]

In the United States, the Office of the Director of National Intelligence's 2023 *Annual Threat Assessment* makes clear the cyber threat posed by the People's Republic of China (PRC): "China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland ... China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems." [15]

As of this date, Russia's unprovoked war of aggression against Ukraine has not gone the way Russia intended and that has taken significant energy away from its cyber attacks elsewhere. As the *Annual Threat Assessment* puts it, "Ukraine war was the key factor in Russia's cyber operations prioritization in 2022. Although its cyber activity surrounding the war fell short of the pace and impact we had expected, Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions."

With cyberspace becoming a focal point for national security, impacting governments, businesses, and individuals globally, it is evident that a comprehensive cybercrime treaty might appear to be a step towards safeguarding all peoples. Russia presented its updated proposal for a United Nations Convention aimed at Ensuring International Information Security to the UN Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG) on March 7, 2023.[16] The Open-Ended Working Group (OEWG) on information and telecommunications in the context of international security is a United Nations (UN) initiative. As of the date of this article in September 2021, the OEWG has been a forum for discussing the peaceful use of ICTs and the prevention of conflicts stemming from their use. Member states of the UN, including Russia, have participated in the OEWG to share their views on norms, rules, and principles of responsible behavior in cyberspace.

[14] Canadian Centre for Cyber Security, "How to Identify Misinformation, Disinformation, and Malinformation," ITSAP.00.300, February 2022, https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300.

[15] *Annual Threat Assessment of the U.S. Intelligence Community* (Office of the Director of National Intelligence, February 6, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[16] "Updated Concept of the Convention of the United Nations on Ensuring International Information Security" (United Nations, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf.

Russia argues that a legally binding treaty is necessary due to perceived deficiencies in existing international law. However, several countries, including Sweden, South Korea, Colombia, Austria, and the United States, hold the view that no such gaps exist. Instead, these countries assert that what is needed is a more precise interpretation and clarification of the existing body of international law. Further, these states argue that should the nine-page Russian proposal garner support within the United Nations, it has the potential to erode the accountability of state actions in cyberspace and pose a significant threat to digital human rights. [17]

A Cloud of Uncertainty

Historically, Russia's perspective on international cybersecurity often diverges from that of many Western nations. Moscow has long advocated for a "sovereign internet" and has supported measures that emphasize state control over information flow.[18] The Russian proposal for a global cybercrime convention reflects this viewpoint and may emphasize state sovereignty in the cyberspace domain. Nonetheless, Russia's active intervention and abuse in Ukraine stand in stark contrast to their own stated diplomatic overtures.[19]

On November 18, 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 benefits from sounding potentially progressive, it has direct negative consequences for the Budapest Convention on Cybercrime[20] 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.

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

[17] Isabella Wilkinson, "What Is the UN Cybercrime Treaty and Why Does It Matter?" *Chatham House*, August 2, 2023, https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter.

[18] Timmy Broderick, "Russia Is Trying to Leave the Internet and Build Its Own," *Scientific American*, July 12, 2023, https://www.scientificamerican.com/article/russia-is-trying-to-leave-the-internet-and-build-its-own/.

[19] Mercedes Page, "The Hypocrisy of Russia's Push for a New Global Cybercrime Treaty," *The Interpreter*, March 7, 2022, https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty.

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

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"[21] may be best understood as primarily political moves to strengthen the Russian goal of establishing "the system of international information security."[22] 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.[23]

Concomitantly, Russian arguments for creating 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[24] 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.

Additionally, some foreign policy experts in Russia justify the goal of 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, become too expensive.[25] Likewise, the demand to pre-install Russian software to "track, filter, and reroute internet traffic"[26] can be read in the contexts of information security, critical infrastructure protection, and boosting national re-

[21] 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/.

[22] "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.

[23] 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.

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

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

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

search and development markets.[27] Demonstrably, widening the coverage of federal (Roskomnadzor's) enforcement mechanisms from routing traffic to all ITC devices also increases political and informational control over individuals.

By weaponizing diplomatic processes, Russia continues to threaten the ethos of an unrestricted internet, hinting at a darker future of a segmented cyberspace dominated by a few influential nations.[28] While technological approaches differ, Russia and China are working in parallel to enforce what many experts maintain is a dystopian, state-control view of cyberspace on the world. This means exercising policies that are in stark contradiction with the democratic order and undercutting the framework of global economic order and commercial interests over the long term.

A new international legal instrument on cybercrime would also duplicate existing work and preempt the conclusions of the open-ended intergovernmental UN expert group (IEG)[29] to conduct a comprehensive study of the problem of cybercrime and responses to it by member states. Furthermore, there is no consensus on the scope that such a new treaty on cybersecurity would have. In addition, Western nations appear to recognize that such a process might also divert efforts from national legislative reforms and current capacity building, essentially throwing a wrench into domestic efforts to curb cybercrime.

In Want of a Progressive Vision for Cyberspace

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[30] and the Paris Call for Trust and Security in Cyberspace.[31] Notably, some experts main-

[27] 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.

[28] Rishi Iyengar, Robbie Gramer, and Anusha Rathi, "Russia Is Commandeering the U.N. Cybercrime Treaty," *Foreign Policy*, August 31, 2023, https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty/.

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

[30] "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.

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

tain the West has not been particularly successful in its efforts to convince and engage states outside its perimeter.[32]

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. In this critical period, it is paramount for democratic countries to unite, re-establish cyberspace standards, and advocate for a cohesive vision for the digital world before it splinters beyond repair.

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.

Acknowledgment

Connections: The Quarterly Journal, Vol. 22, 2023, is supported by the United States government.

About the Author

Sean S. Costigan – see the CV on page 6 of this issue, https://doi.org/10.11610/Connections.22.1.00

[32] 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.