Published in JustSecurity
7 October 2025
Contact: alex.cyber@protonmail.com

Russian Motivations Behind the "Hanoi Convention" Against Cybercrime

Alexander Seger, 7 October 2025

Later this month, governments from around the world will be invited to sign a new international treaty: On Oct. 25, in Hanoi, Vietnam, the "United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes" is to be opened for signature. The treaty is being branded as the "Hanoi Convention."

The cause for its bulky official title is Russia. The lengthy name represents a compromise after Russia objected to using the term "cybercrime." Russia is also the reason why the United Nations General Assembly (UNGA) in December 2019 decided to launch the process that led to this treaty. Russia had introduced UNGA Resolution A/RES/74/247, which established an "Ad Hoc Committee" tasked with negotiating the draft text of a convention. For Russia, the Hanoi Convention is its "baby".

This raises a number of questions: Why would Russia, known as a major source of cybercrime, promote an international agreement against cybercrime? Does Russia have reason to be satisfied with the Hanoi Convention resulting from this process? Could this convention be a game changer in the sense that Russia may finally crack down on cybercrime and engage in international cooperation? If not, what is Russia planning to do with this treaty?

With the opening date for signature approaching and implementation by states to follow thereafter, these questions will come again to the forefront. Governments of democratic countries need to remain alert and understand Russia's motivations behind this new convention.

Russia and Cybercrime

Russia is the single biggest source of cybercrime and has been so for years. Early examples of organized cybercrime include the so-called "Russian Business Network," which, by 2007, had become the largest provider of the criminal infrastructure (internet access, bulletproof hosting) in Russia for activities ranging from phishing and identity theft to malware distribution, fraud scams, child sexual abuse materials, and command and control servers for botnets and distributed denial of service (DDOS) attacks. Another well-known example is the Internet Research Agency, also known as the "Sankt Petersburg troll factory," which was established in 2013 by Yevgeny Prigozhin, a Russian tycoon and founder of the private military company Wagner. In 2018, the Trump administration sanctioned it for interfering with the 2016 U.S. election.

The list of Russian cybercrime activity goes on and on. The waves of cyberattacks against Estonia in 2007, the attacks against Georgia in 2008, the Zeus Trojan malware used to steal banking information, the disruption of Ukraine's power grid in 2015, the NotPetya malware attack of 2016 that targeted Ukraine but spread globally, Evil Corp ransomware attacks in 2019, the SolarWinds Hack in 2020, or the Colonial Pipeline ransomware attack in 2021 are further examples. In fact, most major ransomware groups (Lockbit, Conti, Revil, Ryuk, Hive, Qilin, and others) have been linked with Russia. An increasing number of countries (Estonia, France, Germany, Ukraine, the United Kingdom, and the United States among them) officially attribute cyberattacks to specific Russian State actors.

Furthermore, following Russian cyber interference with the Ukrainian presidential elections in 2014, Russia began to interfere with democratic processes through cybercrime and information operations elsewhere. In addition to the United States, it interfered with the BREXIT referendum in the United Kingdom in 2016, and more recently with elections in Germany (2025), Moldova (2024 and 2025), and Romania (2024 and 2025).

Before it launched its full-scale invasion of Ukraine in February 2022, Russia preceded that aggression with cyberattacks and has continued to wage them throughout the war. The cyber domain is essential to Russian campaigns against other countries as well.

The boundaries between the Russian State and criminal groups are fluid. Institutions of the Russian regime have not only developed a symbiotic relationship with cybercrime groups but have themselves adopted the modus operandi of cybercriminal organizations:

- The regime has created institutions within their security services to carry out cyberattacks and commit cybercrime, that is, within the Russian Federal Security Service (FSB), the Russian Foreign Intelligence Service (SVR) and the Russian General Staff Main Intelligence Directorate (GRU) of the Ministry of Defense. These State actors are also known as APT28/Fancy Bear, APT29/Cozy Bear, Voodoo Bear/Sandworm Team, and by other names.

- The regime supports or outsources activities to other criminal groups or individuals to make use of skilled resources and cybercrime-as-a-service to serve its interests in a targeted and efficient manner. This type of arrangement also provides the Russian regime with "plausible deniability," attributing attacks against foreign targets to "patriotic hackers".

- The regime is tolerant toward cybercrime groups or individual criminals and permits them to pursue their activities as long as these do not target Russian institutions or otherwise do not run counter to the interests of the regime. Broadly speaking, cybercrime groups are fairly free to operate in Russia as long their targets are abroad, preferably in Western countries or in Ukraine.

In short, cybercrime and other forms of cyberthreats committed by security bodies of the Russian State and criminal organizations are often difficult to distinguish from one another. These actors pursue the interests of the Russian regime in one way or another. They appear to have morphed into one criminal organization or network under the

overall direction of the Russian regime. Those organizations that operate in the interest of the regime are provided with a "roof" (*krysha*) and are protected; others may be prosecuted.

Why would Russia promote an international treaty on cybercrime?

Given the role of Russian State and non-State actors in the commission of cybercrime, the question is why Russia would be the main proponent of an international treaty against cybercrime?

Between 2000, when Vladimir Putin first became president of the Russian Federation, and 2022, when the U.N. ad hoc committee began negotiations of what was to result in the "Hanoi Convention," Russia made multiple proposals and concluded several agreements on "information security". These were international offshoots of domestic Russian policies.

In his first month as president, Putin approved a National Security Strategy, and a few months later, in September 2000, he signed off on the first iteration of the "Information Security Doctrine of the Russian Federation." Given his background as an intelligence officer, it was not surprising that for him national security was not possible without information security. The new doctrine was also about controlling the information to which citizens could be exposed to and "preventing illegal informational and psychological influences on the mass consciousness of society."

On Dec. 5, 2016, Putin approved an updated "Doctrine of Information Security of the Russian Federation." Similar to the 2000 version, the new edition was also aimed at establishing full State control over the domestic information space in order to protect Russian citizens against "harmful" information.

These domestic doctrines were accompanied by several regional and international agreements signed by or proposed by Russia:

- In June 2001, an "Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences relating to computer information" was signed in Minsk (Belarus) by Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russian Federation, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan.

- A few years later, in June 2009, Russia joined the "Shanghai Cooperation Agreement" (Agreement between the governments of State members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security) between China, Kazakhstan, Kyrgyzstan, Russian Federation, Tajikistan, and Uzbekistan. The agreement was meant to counter threats such as the distribution of "harmful" information, including information that "distorts the perception of the political system, social order, domestic and foreign policy, important political and social processes in the State, spiritual, moral and cultural values of its population."

- In April 2010, at the United Nations Congress for Crime Prevention and Criminal Justice in Salvador de Bahía (Brazil), Russia lobbied strongly for a U.N. treaty on

cybercrime. Although that attempt failed, an U.N. Intergovernmental Expert Group on Cybercrime was established as a compromise to study the matter. This IEG met seven times between 2011 and 2021, but it reached no agreement on the need and feasibility of a U.N. treaty on cybercrime. This is why Russia went directly to UNGA in 2018 and again in 2019.

- In September 2011, in Yekaterinburg, Russia, the Russian Ministry of Foreign Affairs published a concept for a "Convention on International Information Security" covering measures to prevent and resolve military conflicts, the use of the information space for terrorist purposes and illegal activity – including the "unauthorized dissemination of information" – in the information space.

- In May 2017, during a meeting of the U.N. Commission for Crime Prevention and Criminal Justice (CCPCJ) in Vienna, Austria, Russia organized a special event where it presented a "Draft of the United Nations Convention on Cooperation in Combating Information Crimes." In October 2017, the Russian Ministry of Foreign Affairs submitted a letter, to which an amended "Draft United Nations Convention on Cooperation in Combatting Cybercrime" was appended, to the U.N. Secretary General for circulation to UNGA.

- In July 2021, Russia submitted a new version of the draft entitled "United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" for consideration by the ad hoc committee. At that point, UNGA had adopted Resolution A/RES/74/247 but the treaty process had not commenced yet because of the COVID pandemic.

- In March 2023, Russia submitted its vision for a Convention of the U.N. on Ensuring International Information Security to another U.N. process, the U.N. Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG). Section II of that document indicated what Russia considered the "main threats to international information security."

Earlier, in July 2013, Putin approved a specific policy on international information security, officially titled: "Fundamentals of the State Policy of the Russian Federation in the Area of International Information Security for the Period until 2020." That policy was to address major threats related to the use of information and communication technology. One of the tasks identified under this policy was the:

> (a) Promotion in the international arena of the Russian initiative to develop and adopt, under the auspices of the United Nations, a Convention on Cooperation in Combating Information Crime, and intensify work with the member States of the Shanghai Cooperation Organization, the member States of the Commonwealth of Independent States, the member States of the Collective Security Treaty Organization and the BRICS member States to support this initiative.

In April 2021, Putin approved an updated version of these "fundamentals." Tasks now included facilitating the work of the U.N. Ad Hoc Committee and the creation of the conditions for the subsequent adoption of the U.N. convention.

After assessing this flurry of activity, it is clear that the promotion of a U.N. treaty against cybercrime was not driven by a desire on the part of Russia to take effective measures and engage in international cooperation against cybercrime. Instead, the

primary driver was and is the promotion of a system of "international information security" modelled on the Russian approach. Under this system, it is governments that exercise sovereign control of their country's information space, protect this space against external interference, and ensure that individuals are exposed to what they consider reliable information only.

In the first session of the ad hoc committee (in New York in early 2022), the representative of Russia underlined the core principles that should guide the future treaty. Speaking on behalf of Russian Foreign Minister Sergey Lavrov, he listed the sovereignty of States, non-interference in their internal affairs and protection of human rights. His statement was made four days after Russia had commenced its full war of aggression against Ukraine. Therefore, most participants in the session perceived the statement as highly cynical.

Russia's limited interest in actual measures against cybercrime is also illustrated by another fact: While Russia signed the 2001 CIS agreement and then joined or proposed other treaties, what Russia did not sign was the Council of Europe's Convention on Cybercrime that was opened for signature in November 2001 in Budapest, Hungary (hence the "Budapest Convention"). At the time, Russia was a member of the Council of Europe (February 1997 – March 2022) and had participated in the preparation of that Convention between 1997 and 2001.

More than that: from 2004 onwards, the Russian Ministry of Foreign Affairs actively agitated against this treaty, quoting threats to national sovereignty caused by its Article 32 on transborder access to data, a provision that had previously been agreed upon at a G8 Ministers of Justice and Interior meeting in Moscow in October 1999. There is not enough space here to explain the arguments and debates of the past 25 years, but the short version is that Russian claims regarding Article 32 have been refuted.

The actual reasons for not joining the Budapest Convention were rather that (a) the majority of States that had joined this treaty did not subscribe to Russia's political vision of information control and "cyber sovereignty," and (b) that Russia was not particularly interested in effective mechanisms for cooperation on cybercrime.

Instead, Russia set out to promote a U.N. treaty not on "cybercrime" but on the use of information and communication technologies for criminal purposes; a treaty that was to replace the "outdated" Budapest Convention.

Did Russia achieve its objectives?

When UNGA adopted the convention against cybercrime on Dec. 24, 2024, Russia may have partially achieved its objective of having the U.N. for the first time agree on a legally binding treaty related to "information and communication technology" other than the International Telecommunications Regulations (as updated in 2012 but not universally accepted). Russia fought hard in the ad hoc committee to have the notion of "information and communication technology systems" in the title of the treaty (hence the awkward official title).

The "Hanoi Convention," however, is not the type of information control treaty that Russia tried to obtain. The numerous human rights and rule of law safeguards incorporated in the convention are setting a precedent for future U.N. criminal justice

treaties. Russia sided with Iran's unsuccessful attempts to have those safeguards voted out of the text. Most other Russian submissions for text and provisions were also rejected.

The backbone of the "Hanoi Convention" (offenses, investigative powers, international cooperation on cybercrime and electronic evidence) consists of provisions copied from the Budapest Convention on Cybercrime. Rather than declaring that convention obsolete, the U.N. treaty thus affirms its continued relevance. At the same time, the new tools for cross-border disclosure of electronic evidence of the Second Protocol to the Budapest Convention (opened for signature in 2022) have not been included in the Hanoi Convention. Given the new mechanisms of the Second Protocol as well as the attention paid to the Budapest Convention during the U.N. treaty process, interest and membership in that convention surged considerably since 2022. If Russia intended to disrupt the functioning of the framework of the Budapest Convention on Cybercrime through the U.N. treaty process, Russia not only failed but achieved the contrary.

The idea that Russia, leading a sovereigntist camp of authoritarian countries, would define the direction of the U.N. treaty process also did not materialize. The outcome of the process was largely determined by a coalition of democratic countries (mostly States aligned with the Budapest Convention) that had insisted on a narrow criminal justice treaty, consistent with the Budapest Convention and with the human rights and rule of law safeguards necessary for international cooperation.

In short, although the U.N. treaty against cybercrime is now here because of Russia, and although Russia will likely spin the adoption of the Hanoi Convention as a political win, it is certainly not the treaty that Russia wanted.

What next: what will Russia do with the Hanoi Convention?

The game is not over. In 2027, Russia will have another opportunity to try again: during the treaty process, Russia kept insisting on a long list of additional offenses to be included in the convention ("incitement to subversive or armed activities", "extremism-related offenses", etc.). A compromise had to be found, and so when UNGA adopted the treaty in December 2024 through Resolution 79/243, it also decided to launch the negotiation of "a draft protocol supplementary to the Convention, addressing, inter alia, additional criminal offences as appropriate." Two years after the adoption of the treaty, Russia will attempt again to obtain international support for its position.

In spite of the numerous safeguards in the Hanoi Convention, there are risks for misuse. The Russian regime may use this convention for domestic and transnational repression of dissent (as it did with other treaties in the past). It may also use provisions on asset forfeiture, fraud, money laundering, corporate liability or on participation and attempt to target assets of multinational service providers (accused of "neo-colonialism" by Russian representatives during the committee process).

The purpose of the Hanoi Convention is to strengthen international cooperation on cybercrime and electronic evidence. The prospects are slim that Russia will take firm action against cybercrime domestically and engage in international cooperation in good faith once the Hanoi Convention is in force. The Russian regime is not known for honoring its international commitments.

In any case, Russia – being the most significant source of cybercrime globally – would not have needed to await an international treaty to take domestic action in order to prevent State institutions and other criminal organizations from committing cybercrime (or from making or carrying out those other threats listed in its proposal for a convention on international information security).

In conclusion, the Hanoi Convention will be useful for cooperation with and among countries that are not already part of the framework of the Budapest Convention. It will have little impact, however, on Russian cybercrime. Russia's push for a U.N. treaty was never motivated by an intention to take firm action on cybercrime but was and is part of a broader campaign to bring internet governance under the control of sovereign States, to control information and suppress dissent, and to expand international support for Russia's positions. Its campaign will continue, but if the coalition of countries around the Budapest Convention holds and remains engaged, Russia will not have its way. And perhaps the oversight mechanism of the Hanoi Convention could be used to expose the actions of the Russian regime in cyberspace.

Editor's note: From February 1999 to September 2025, the author was with the Council of Europe, including as the Executive Secretary of the Cybercrime Convention Committee (www.coe.int/cybercrime) and responsible for the framework of the "Budapest Convention". In that function he also participated and facilitated common positions of the parties to the Budapest Convention in the United Nations treaty process leading to the "Hanoi Convention". He has been interacting with Russian authorities in matters related to cybercrime, corruption, money laundering and organized crime for more than twenty years. The views expressed here are those of the author.