The UN Cybercrime Treaty: A Trojan Horse for Suppressing Dissent

By Dr. Ivana Stradner and Emily Hester

October 23, 2025

Executive Summary

Not content to only suppress human rights in their own countries, Russia and China are exporting oppression around the world and using the United Nations as legal cover. On December 24, 2024, the United Nations General Assembly adopted the Convention Against Cybercrime.[1] While ostensibly intended to enhance international cooperation to address cybercrime,[2] the treaty is actually a platform for authoritarian states to advance ideas about state control of the internet, rope democratic governments into complicity with repression, and weaken key cybersecurity tools on which Americans depend.

The treaty's overly broad yet still vague definition of cybercrime and its emphasis on mutual assistance mean Russia could potentially use its terms to force Washington to acquiesce to or even assist Moscow's own trumped-up criminal prosecutions. While the United States is unlikely to ratify the treaty, it voted[3] in support of its final text and later voiced support for its formal adoption, opening the door for its entrance into international law. The United Nations is hosting a signing ceremony in Hanoi on October 25-26.[4] Only those that ratify the treaty will be obliged to follow it, but the ability to cite a multilateral standard will enable ratifying states to exert pressure on others.

The treaty's trajectory follows China and Russia's escalating cyber aggressions towards the U.S. and its allies. China's "Volt Typhoon" cyberattack gave China unprecedented access to U.S. water, electricity, and critical infrastructure, providing them valuable information to compromise key U.S. response systems.[5] Yet, at the same time, these malign actors claim to be leading the charge in crafting a safer international cyberspace with the UN treaty.

1. United Nations General Assembly Resolution 79/243, December 24, 2024. (https://www.unodc.org/unodc/en/cybercrime/convention/home.html)
2. United Nations General Assembly, "Statement attributable to the Spokesperson for the Secretary-General — on the adoption of the United Nations Convention against Cybercrime," December 24, 2024. (https://www.un.org/sg/en/content/sg/statement/2024-12-24/statement-attributable-the-spokesperson-for-the-secretary-general-the-adoption-of-the-united-nations-convention-against-cybercrime)
3. United Nations, Office on Drugs and Crime, Press Release, "Member States finalize a new cybercrime convention," August 9, 2024. (https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html)
4. "Hanoi to host signing ceremony of UN Convention against cybercrime," *Vietnam News*, October 11, 2025. (https://news.tuoitre.vn/hanoi-to-host-signing-ceremony-of-un-convention-against-cybercrime-10325101017483961 4.htm)
5. Jack Burnham and Johanna Yang, Public Comment to the Federal Communications Commission, "Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control," *Foundation for Defense of Democracies*, July 21, 2025. (https://www.fdd.org/wp-content/uploads/2025/07/FCC-Comment-July_Transparency-Adversary-Control-Burnham-Yang.pdf)

Washington cannot undo the passage of the cybercrime treaty. Instead, the United States must prepare the Department of Justice to withstand authoritarian attempts to leverage the treaty to compel U.S. assistance in suppressing dissent. Washington must also strengthen its cyber diplomacy capabilities within the State Department to thwart further attempts by Russia and China to shape multilateral cyber laws and norms. Finally, the United States must push back, promoting instead an earlier cybercrime agreement, the Budapest Convention, that aligns with U.S. interests and affirms democratic values. To advance human rights online and freedom of expression safeguards around the world, the United States and its allies must confront digital authoritarianism, even when it takes the form of a multilateral treaty.

Digital Sovereignty and the Genesis of the Treaty

The UN cybercrime treaty is the culmination of nearly a decade of persistent Russian — and later, Chinese — efforts to change existing international law. As these two nations increased exports of intrusive surveillance technology and other tools of repression, they rallied dozens of undecided nations to their cause. The United States, meanwhile, ceded the battlespace and then ultimately lent its approval, fearing that opposing the treaty would only undermine U.S. influence further.[6]

Previously, the primary international mechanism defining cybercrime and encouraging interstate cooperation to combat it was the 2001 Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention. This convention affirms an individual's freedom of expression and right to privacy. While it boasts 81 members, including the U.S., China, Russia, and other countries with problematic human rights records have refused to sign it since few developing countries were involved in drafting.[7] By putting forward a new treaty, Moscow, Beijing, and their partners hope to eclipse the Budapest Convention, which countries continue to use to develop domestic laws and facilitate international cooperation.[8]

Russia has been attempting to ingrain the concept of digital sovereignty in international forums since 2012, when large-scale anti-government protests demanding political reforms, largely coordinated online, swept the nation.[9] Digital sovereignty holds that a government should be able to control the internet that its citizens use. For leaders like Russian President Vladimir Putin, digital sovereignty means shaping a domestic information space completely severed from the global internet and fully subject to state surveillance.[10] Consistent with standard UN procedure, the Kremlin presented a letter for circulation to the United Nations General Assembly containing the first draft of what would become the UN's cybercrime treaty.[11]

6. Suzanne Smalley, "UN cybercrime treaty lead negotiator: US will suffer if it doesn't vote yes," *The Record*, October 7, 2024. (https://therecord.media/un-cybercrime-treaty-lead-negotiator-us-must-pass)
7. Elizabeth Dominic, "The debate over internet governance and cyber-crimes: West vs the rest?" *The Centre for Internet & Society*, June 8, 2020. (https://cis-india.org/internet-governance/blog/the-debate-over-internet-governance-and-cyber-crimes-west-vs-the-rest)
8. Council of Europe, "Joining the Convention on Cybercrime: Benefits," July 9, 2025. (https://rm.coe.int/cyber-buda-benefits-2025-9-july-en/1680b6b132)
9. Alexandra V. Orlova, "'Digital Sovereignty.' Anonymity and Freedom of Expression: Russia's Fight to Re-Shape Internet Governance," *UC Davis Journal of International Law & Policy*, Vol. 26, No. 2, Spring 2020, pages 225-248. (https://jilp.law.ucdavis.edu/archives/26/2/digital-sovereignty-anonymity-and-freedom-expression-russias-fight-re-shape-internet)
10. Arun Sukumar and Arindrajit Basu, "Back to the Territorial State: China and Russia's Use of UN Cybercrime Negotiations to Challenge the Liberal Cyber Order," *Journal of Cyber Policy*, October 24, 2024. (https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2436591)
11. United Nations General Assembly, "Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General," October 16, 2017. (https://digitallibrary.un.org/record/1327693?ln=en&v=pdf)

In 2018, as Moscow was first starting to rally support, Russia submitted a request that the UN establish an Open-Ended Working Group (OEWG) on Information and Communication Technologies. The OEWG was open to any interested UN member states, with the stated intent of making the UN negotiation process "more democratic, inclusive and transparent."[12]

The United States proposed a competing approach to UN discussions about technology and security issues, forming a 25-state Group of Governmental Experts (GGE).[13] GGEs are a common structure within the UN to study issues of concern, but the OEWG, by virtue of its more inclusive approach, became the de facto group making decisions and amendments to the drafted treaty. The GGE, meanwhile, remained more of an observer group.

In 2019, China, Russia, and several of their allies took the next typical step toward a UN treaty by proposing a General Assembly resolution calling for an international convention to combat cybercrime based on Russia's initial draft. The resolution passed by a vote of 79 to 60 with 33 abstentions, with the United States, the European Union, and other democracies voting no.[14] A month later, the General Assembly took the usual step of creating an ad hoc committee (AHC) comprised of member states, nonmember state observers like the European Union, and civil society organizations to begin the drafting process. While the AHC planned to hold its first meeting in the summer of 2020, the COVID-19 pandemic delayed it until 2021.[15]

From 2021 to 2024, six AHC negotiation sessions took place. Throughout the fraught process, the principal complaints democracies lodged against the draft remained the same: its overly broad scope and lack of human rights protections. There was a lack of consensus around the definition of "cybercrime,"[16] with Russia and China pushing for a broad definition to include content-related crimes, such as incitement of terror, disinformation, extremism, and subversion.[17] Without precise definitions of such terms in the UN treaty, human rights experts warned at the time, authoritarian nations would use the treaty to criminalize all dissent by arbitrarily branding it as disinformation or one of the other prohibited activities.[18] A narrower definition of cybercrime would have focused on unauthorized access to computer systems. The Budapest Convention, for example, focuses on preventing illegal

12. United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," December 5, 2018. (https://docs.un.org/en/A/RES/73/27)

13. Heli Tiirmaa-Klaar, "The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body," *The Hague Centre for Strategic Studies & Global Commission on the Stability of Cyberspace*, December 2021. (https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf); United Nations, "General Assembly Resolution 73/266 Advancing responsible State behaviour in cyberspace in the context of international security," December 22, 2018. (https://docs.un.org/en/A/RES/73/266)

14. Edith M. Lederer, "UN gives green light to draft treaty to combat cybercrime," *The Associated Press,* December 27, 2019. (https://apnews.com/general-news-79c7986478e5f455f2b281b5c9ed2d15)

15. Karen Gullo and Katitza Rodriguez, "UN Cybercrime Treaty Timeline," *Electronic Frontier Foundation*, accessed October 13, 2025. (https://www.eff.org/pages/un-cybercrime-treaty-timeline)

16. United Nations, Second session of Ad Hoc Committee on Cybercrime, "U.S. Remarks on Criminalization Chapter," May 30, 2022. (https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/USA_Ciminialization.pdf); United Nations, Office on Drugs and Crime, Second session of the Ad Hoc Committee, May 30-June 10, 2022. (https://www.unodc.org/unodc/cybercrime/ad_hoc_committee/ahc-second-session.html)

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. Madeline Earp, "Why the UN's push for a cybercrime treaty could imperil journalists simply for using the internet," *Committee to Protect Journalists*, January 18, 2022. (https://cpj.org/2022/01/why-the-uns-push-for-a-cybercrime-treaty-could-imperil-journalists-simply-for-using-the-internet)

access to computer systems, illegal interception of nonpublic data transmissions, data and system interference, fraud, and forgery.[19]

Russia and China strengthened cooperation with potential supporters via international partnerships and trade. Since 2015, but with greater intensity in recent years, China has been mounting a diplomatic campaign to build its Community with a Shared Future in Cyberspace, an association that seeks to rally like-minded states around a pro-sovereignty vision for global cyberspace.[20] Meanwhile, Chinese technology companies whose products are well-equipped to support state surveillance and censorship are finding receptive buyers among African governments.[21] These commercial relationships then feed back into China's diplomatic efforts to promote its vision of the internet. China has not published the membership list of its Community with a Shared Future in Cyberspace; however, an acceleration in cyber cooperation agreements among regional alliances such as Brazil, Russia, India, China, and South Africa and the Shanghai Cooperation Organization over the past two years indicates China's progress in rallying support for its vision of sovereign cyberspace.[22]

Russia, meanwhile, has already been introducing interested states to its System for Operative Investigative Activities (SORM), its mass communications surveillance system.[23] Unlike in the West, where judicial warrants are required for targeted surveillance, Russian telecommunications operators automatically give the state's security agency a backdoor into all internet communications. Security services in Kazakhstan, Kyrgyzstan, and Belarus now use "SORM-style systems," and Russia has exported this capability to clients ranging from the Gulf monarchies to leftist Latin American regimes such as Cuba and Venezuela.[24]

These commercial and diplomatic efforts are bearing fruit. Countries that were initially opposed to the treaty, such as Brazil, changed their tune. Other countries that were considered swing voters, like Indonesia, Mexico, Singapore, and South Africa, ultimately supported the treaty.

During this same time, the United States failed to make meaningful changes to the draft text or to rally opposition against its passage. By the summer of 2024, participating UN member states agreed on the treaty's final text.[25] In

19. Council of Europe, "Convention on Cybercrime," November 23, 2001. (https://rm.coe.int/1680081561)
20. Dakota Cary, "Community watch: China's vision for the future of the internet," *Atlantic Council*, December 4, 2023. (https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet); Nathan Attrill and Audrey Fritz, "China's cyber vision: How the Cyberspace Administration of China is building a new consensus on global internet governance," *Australian Strategic Policy Institute*, November 24, 2021. (https://www.aspi.org.au/report/chinas-cyber-vision-how-cyberspace-administration-china-building-new-consensus-global)
21. Samuel Hoffman, "Potential Chinese Influence on African IT Infrastructure," *Censys*, March 8, 2023. (https://censys.com/blog/potential-chinese-influence-on-african-it-infrastructure)
22. Dakota Cary, "Community watch: China's vision for the future of the internet," *Atlantic Council*, December 2023. (https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet); Đorđe Krivokapić, "A Disturbing Marriage: Serbia and China Team Up on Digital Surveillance," *Center for European Policy Analysis*, January 27, 2022. (https://cepa.org/article/a-disturbing-marriage-serbia-and-china-team-up-on-digital-surveillance)
23. "Lawful interception: the Russian approach," *Privacy International*, March 4, 2013. (https://privacyinternational.org/blog/1296/lawful-interception-russian-approach)
24. Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *Brookings Institution*, August 2019, page 10. (https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf)
25. "United Nations: Member States Finalize a New Cybercrime Convention," *UNODC*, August 2024. (https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html)

November, when the United Nations held its final meeting on the treaty, the United States and its allies vocally endorsed the final text, paving the way for the final December vote.[26]

At least part of the United States' failure can be attributed to how the State Department chose to engage in the process. Compounding the mistake of not including developing nations in the GGE, State failed to bring the right experts to the table to represent U.S. interests in the negotiations. The U.S. negotiators hailed from the Bureau of International Narcotics and Law Enforcement Affairs (INL). Unlike INL, State's Bureau of Cyberspace and Digital Policy has extensive expertise in cyber diplomacy, regularly coordinating with allies and partners to build cyber resilience.[27] Without this critical expertise, the U.S. representatives mistakenly prioritized the largely symbolic win of participating in international cooperation over the critical need to prevent the UN cybercrime treaty from passing. The INL negotiators defended their support for the final text on the grounds that it is better to be able to influence the treaty's implementation and evolution than vote against the treaty and risk not being able to participate.[28] Senior State Department officials accepted this rationale and approved the decision to support the treaty's adoption.[29]

The Damage the Treaty Will Do

Fragmentation of the global internet into sovereign internet ecosystems is an affront to the open, free, and secure internet that has been a touchstone of democratic values in the digital age. By cementing protections for digital sovereignty, Russia, China, and their partners are seeking to remove critical human rights protections and threatening to make democratic signatories complicit in their trumped-up prosecutions of journalists and dissidents.

Warnings to this effect came from both business leaders and political figures. In January 2024, the Cybersecurity Tech Accord, representing 177 technology and cybersecurity companies, submitted a statement to the AHC arguing that the draft was not fit for purpose because it would make cyberspace less secure and undermine human rights. The statement proposed changes to the draft, noting its current iteration "risk[s] criminalization of a wide range of legitimate online activities" due to overly broad purpose and scope."[30] The statement proposed "minimum necessary changes," including adding "criminal intent" to all articles concerning criminalization and establishing exemptions and an "enabling environment" for good-faith cybersecurity research.[31] The leaders argued that states should decline to ratify it if the changes are not made.[32]

26. Jonathan Greig, "Controversial UN cybercrime treaty clears final hurdle before full vote as US defends support," *The Record*, November 12, 2024. (https://therecord.media/un-cybercrime-treaty-clears-vote)
27. Annie Fixler, "Shaping the Future of Cyber Diplomacy," *Testimony before the House Foreign Affairs Subcommittee on Europe*, April 29, 2025. (https://www.fdd.org/analysis/2025/04/29/shaping-the-future-of-cyber-diplomacy)
28. Suzanne Smalley, "UN cybercrime treaty lead negotiator: US will suffer if it doesn't vote yes," *The Record*, October 7, 2024. (https://therecord.media/un-cybercrime-treaty-lead-negotiator-us-must-pass)
29. Deborah McCarthy, "UN Cybercrimes Treaty Negotiations," *Washington Foreign Press Center*, June 27, 2024. (https://2021-2025.state.gov/briefings-foreign-press-centers/un-cybercrimes-treaty-negotiations)
30. Cybersecurity Tech Accord, "Cybersecurity Tech Accord Submission to the Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime," January 2024. (https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Multi-Stakeholders/Cybersecurity_Tech_Accord_-_7th_AHC_session_submission.pdf)
31. Ibid.
32. Ibid.

In October 2024, six U.S. senators wrote a letter to the Biden administration urging the State Department to reject the treaty.[33] The letter pointed to specific problems around privacy and surveillance, censorship and freedom of expression, and cybersecurity research. It warned that the treaty requires countries to "adopt laws that allow their authorities to force any person or company to facilitate" government access to private data and to "collect and share private internet user data with other countries."

The treaty's definition of a cybercriminal is at the root of these deficiencies.[34] Arguably, the treaty legitimizes domestic laws in authoritarian countries that criminalize speech and peaceful assembly. For example, the text provides wide deference to states to prosecute any cybercrime the state deems serious — defined in the treaty as "constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty" under each nation's own laws. This covers Russian laws like those that prescribe up to 15 years imprisonment for criticizing the war in Ukraine.[35]

While the text includes superficial nods to protecting human rights, other passages undermine this commitment.[36] Under article 6, the treaty advises parties to "ensure" its implementation "is consistent with their obligations under international human rights law." The article states the treaty cannot "be interpreted as permitting suppression of human rights or fundamental freedoms" such as freedom of expression "in a manner consistent with applicable international human rights law."[37] This language, however, effectively permits countries to decide for themselves what might be considered "applicable" international law. In contrast, the Budapest Convention's article on human rights requires implementation consistent with the UN's 1966 International Covenant on Civil and Political Rights, which includes extensive protections for freedom of speech and due process.[38]

Meanwhile, article 5 also affirms the document's prioritization of state sovereignty over adherence to any international legal instruments. It emphasizes that "obligations" under the treaty should be interpreted "in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States."[39] This article, absent from the Budapest Convention, allows states to violate international human rights law and blocks other states from intervening, effectively rendering article 6 unenforceable.

33. Suzanne Smalley, "Six senators tell Biden administration UN cybercrime treaty must be changed," *The Record*, October 29, 2024. (https://therecord.media/un-cybercrime-treaty-democratic-senators-seek-changes); Senators Ron Wyden, Tim Kaine, Chris Van Hollen, and Edward J. Markey, *Letter regarding the UN Cybercrime Convention to Secretary of State Anthony Blinken, Attorney General Merrick Garland, Secretary of Commerce Gina Raimondo, and Assistant to the President for National Security Affairs Jake Sullivan*, October 29, 2024. (https://www.documentcloud.org/documents/25257141-wyden_un_convention_against_cybercrime_letter)

34. United Nations Ad Hoc Committee (AHC), "Open Letter from Civil Society and Industry Stakeholders on the Final Draft of the Convention on Cybercrime," August 8, 2024. (https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Final_Draft_Cybercrime_Convention_-_Multistakeholder_Statement.pdf)

35. "Censorship of Anti-War Protest in Russia," *Amnesty International*, accessed October 13, 2025. (https://www.amnesty.org/en/projects/anti-war-protest-in-russia)

36. Anja P. Jakobi and Lena Herbst, "Between a Rock and a Hard Place: the UN Cybercrime Convention," *PRIF Blog*, December 9, 2024. (https://blog.prif.org/2024/12/09/between-a-rock-and-a-hard-place-the-un-cybercrime-convention); Karen Gullo, "Broad Scope Will Authorize Cross-Border Spying for Acts of Expression: Why You Should Oppose Draft UN Cybercrime Treaty," *Electronic Frontier Foundation*, August 1, 2024. (https://www.eff.org/deeplinks/2024/08/overbroad-scope-will-authorize-cross-border-spying-acts-expression-why-you-should)

37. United Nations General Assembly, "United Nations Convention Against Cybercrime," December 24, 2024. (https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en)

38. Council of Europe, "Convention on Cybercrime," November 23, 2001. (https://rm.coe.int/1680081561)

39. United Nations, "Draft text of the Convention," Article 5, September 1, 2023, page 18. (https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_01.09.2023_PM.pdf)

In practice, these flaws in the treaty threaten existing mechanisms for international legal cooperation. The United States uses Mutual Legal Assistance Treaties (MLATs) to establish how and when it cooperates with foreign partners on law enforcement investigations, including how the two sides will exchange evidence, such as electronic data.[40] MLATs contain provisions articulating when the Department of Justice will refuse to cooperate, particularly when there are concerns about human rights violations. The United States holds MLATs with aggressors like Russia and China, although it refuses to sign MLATs with Iran and other countries with which it has no diplomatic relations.

The Justice Department's Office of International Affairs (OIA) must respond to each mutual assistance request it receives.[41] A rise in cybercrime has bombarded the OIA with requests for assistance, "straining resources and slowing response times," according to the department.[42] While the treaty acknowledges the existing precedent of MLATs, it argues parties should "afford one another the widest measure of mutual legal assistance … in relation to the offences established in accordance with this Convention … as well as of serious crimes."[43] Cybersecurity and national security lawyers Andrew Adams and Daniel Podair maintain that this language "will undoubtedly complicate the Justice Department's ability to push back on bad-faith requests." They warn that countries requesting assistance from the United States will argue that their requests "have a clear basis under international law — international law of which the United States [has become] a willing supporter" by virtue of its UN vote, even if it never officially ratifies the treaty.[44] At its worst, this increased challenge to the already-strained OIA could result in the Justice Department acquiescing to some of the requests out of an inability to fight every battle or a decision to trade its assistance for agreement from the other party on an unrelated issue.[45]

Additionally, U.S. allies that do become parties to the treaty will face increased pressure to assist bad-faith investigations. For instance, law enforcement authorities and courts in Europe may be more inclined to defer to a UN document even if it results in human rights abuses.

A second problem arising from the cybercrime treaty is of direct concern to technology and cybersecurity firms, many of which oppose the treaty's blanket criminalization of all unauthorized access to computer systems without carve-outs for good-faith research efforts. Today's cybersecurity ecosystem relies on penetration testing, red teaming, and independent researchers responsibly identifying cybersecurity vulnerabilities so that they can be fixed. The six senators noted in their letter that Department of Justice guidelines say that the federal government will not prosecute good-faith security researchers because "computer security research is a key driver of improved cybersecurity."[46] Artificial Intelligence (AI) systems similarly use simulated attacks to identify problems in their models. In contrast, article 7 on "illegal access" defines as punishable any "intentional" access to "an information

40. Mark Jaycox and Lee Tien, "Reforms Abound for Cross-Border Data Requests," *Electronic Frontier Foundation*, December 27, 2015. (https://www.eff.org/deeplinks/2015/12/reforms-abound-cross-border-data-requests)
41. Department of Justice, "Frequently Asked Questions Regarding Legal Assistance in Criminal Matters," April 2022. (https://www.justice.gov/criminal/criminal-oia/file/1498811/dl?inline=)
42. Department of Justice, "The Purpose and Impact of the CLOUD Act- FAQs," accessed October 13, 2025, page 12. (https://www.justice.gov/criminal/media/999616/dl?inline)
43. United Nations, "United Nations Convention against Cybercrime," accessed October 13, 2025, page 29. (https://treaties.un.org/doc/Treaties/2024/12/20241224%2001-27%20PM/Ch_XVIII_16.pdf)
44. Andrew C. Adams and Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare*, December 9, 2024. (https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention)
45. Ibid.
46. Senator Ron Wyden, "Letter on the UN Convention against Cybercrime," *United States Senate*, October 29, 2024. (https://www.documentcloud.org/documents/25257141-wyden_un_convention_against_cybercrime_letter)

and communications technology system without right,"[47] with no exception for responsible and critical security research. Amy Hogan-Burney, a lawyer with Microsoft, warned that the text fails to protect "lawful cybersecurity work that keeps the digital ecosystem secure," such as identifying flaws and testing cybersecurity defenses.[48]

This may dampen critical research into software vulnerabilities to malicious actors and the necessary solutions, leaving systems less secure as a result. The security research community is international. In a 2024 open letter to government officials, HackerOne — a company that hosts bug bounty programs and connects companies with ethical hackers — warned that because of the treaty, "Security researchers operating in or collaborating with entities in countries with fewer protections for good faith security research may find themselves at heightened risk of potential legal consequences for activities that are both ethical and essential to maintaining global cybersecurity."[49]

Policy Recommendations

Over the long term, wrenching UN processes out of authoritarian hands requires a broader reform of UN institutions.[50] In the short and medium term, however, Washington must prepare to withstand the damage of the new UN cybercrime treaty and better advocate for U.S. interests on cybersecurity and internet freedom issues.

1. **Fortify the Department of Justice for an influx of bad-faith MLAT requests:** The Department of Justice should issue internal guidance and prepare procedures to abide by existing MLATs. The department should refuse to entertain requests that it would have previously rejected out of hand. The department should also work with its counterparts in Europe and other democracies to ensure these countries are similarly prepared to withstand an onslaught of requests for evidence and data that will be used to prosecute journalists, dissidents, and human rights activists in authoritarian countries. Furthermore, the department should consider amending existing MLATs with authoritarian countries by inserting language explicitly stating America's deference to the Budapest Convention when reconciling international and domestic procedures. The attorney general should also issue clear guidance to the legal community that the UN treaty holds no weight in U.S. deliberations.
2. **Empower State's Bureau of Cyberspace and Digital Policy to lead international cyber negotiations at the United Nations and in other international forums:** With the passage and likely ratification of the UN cybercrime treaty, Russia and its allies are no doubt emboldened to continue exploiting the UN as a vehicle to embed their authoritarian interests in international norms. Russia has already presented a new proposal to the UN to implement a framework to prevent "political provocations" committed via information technology, such as America's supposed hybrid warfare against the Kremlin. Like the cybercrime treaty, the proposal seeks to further ingrain the framework of digital sovereignty in international cyberspace governance, which will offer states more latitude in cross-border surveillance and further degrade protections for good-faith research and

47. United Nations General Assembly, "United Nations Convention against Cybercrime," December 2024, Article 7. (https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf)
48. Amy Hogan-Burney, "We Need to Fight Cybercrime, Increase State Surveillance," *Microsoft On the Issues*, August 29, 2023. (https://www.linkedin.com/pulse/we-need-fight-cybercrime-increase-state-surveillance)
49. Greg Otto, "HackerOne urges U.S. to advocate for research protections in UN cybercrime treaty," *CyberScoop*, November 14, 2024. (https://cyberscoop.com/un-cybercrime-treaty-hackerone-letter-security-research)
50. Alan Goldsmith, "The Urgent Need for UN Reform," *Foundation for Defense of Democracies*, April 5, 2024. (https://www.fdd.org/analysis/2024/04/05/the-urgent-need-for-un-reform)

human rights.[51] So as not to make the same mistakes again in UN negotiations, the secretary of state should designate the Bureau of Cyberspace and Digital Policy as the lead negotiator in future settings and ensure that other bureaus, as well as the U.S. mission to the United Nations, defer to cyber experts on issues of international cyber law. The White House should also nominate a new ambassador-at-large for cyber to lead the bureau, which has been without a Senate-confirmed appointee since the start of the Trump administration.

3. **Rally support behind the Budapest Convention and oppose the implementation of the UN cybercrime treaty:** Russia, China, and their allies are portraying the UN cybercrime treaty as a replacement of the Budapest Convention, but Washington need not adopt this frame. Instead, the United States should continue to encourage additional countries to sign onto the Budapest Convention, emphasizing the longevity of the document and the plethora of non-European signatories. At the same time and in all relevant forums, U.S. diplomats should highlight the failings of the UN cybercrime treaty, contrasting its permissive attitude towards human rights abuses with the Budapest Convention's strong protections.
4. **Reassert American opposition to authoritarian initiatives at the United Nations:** A major takeaway from the treaty's success is that Russia and like-minded countries perceive international organizations as key forums in which to rally support for and legitimize their efforts to reshape cyberspace.[52] Petr Litvishko, deputy head of Russia's international legal cooperation directorate, argued in 2024 that the cybercrime treaty represents "a new universal instrument at our disposal" to conduct what he described as "professional, intense and painstaking work to combat information crime" vis-a-vis "the block of 'unfriendly' states" — meaning the United States and its allies.[53] This is the true intent behind the treaty. Washington should reassert itself as a voice of opposition in the General Assembly, and rally allies and like-minded parties to do the same.

Conclusion

Addressing cybercrime is critical in today's interconnected world, but an international framework must be crafted with care to safeguard against abuse and protect human rights. The ongoing struggle for freedom of information stands as a formidable challenge to autocratic regimes, which depends on complete control of the information atmosphere. The entry into force of the UN cybercrime treaty is a failure of the United States and its allies to prevent authoritarian states from weaponizing international law for their geopolitical and ideological benefit.

51. Mark Montgomery, "Previewing the UN General Assembly," *Foundation for Defense of Democracies,* September 19, 2025. (https://www.fdd.org/analysis/2025/09/19/previewing-the-un-general-assembly); Anton Denisenko, "Russia Presented a Draft Concept for International Information Security to the UN," *C News* (Russia), February 7, 2025. (https://www.cnews.ru/news/top/2025-02-07_rossiya_predstavila_v_oon)

52. Justin Sherman and Mark Raymond, . "The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom," *The Washington Post*, December 4, 2019. (https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom)

53. Petr Litvishko, "The First Global Treaty Against Cybercrime: From Geopolitical Confrontation to Professional Compromise," *The International Affairs*, Issue 11, 2024. (https://interaffairs.ru/jauthor/material/3090)

About the Foundation for Defense of Democracies

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based, nonpartisan policy institute focusing on foreign policy and national security. For more information, please visit www.fdd.org.

FDD's Center on Cyber and Technology Innovation

FDD's Center on Cyber and Technology Innovation (CCTI) seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities to national security posed by the rapidly expanding technological environment.

FDD's International Organizations Program

Every year, the U.S. Congress appropriates billions of dollars to the United Nations, international organizations, international financial institutions, regional organizations, and multilateral development banks. These contributions are often provided with little or no U.S. oversight and without a comprehensive strategy to advance U.S. interests. FDD's International Organizations Program leverages FDD's regional and subject matter expertise within its centers on American power to identify ways the United States can more strategically employ its resources.

Dr. Ivana Stradner serves as a research fellow with FDD's Barish Center for Media Integrity. She studies Russia's security strategies and military doctrines to understand how Russia uses information operations for strategic communication, especially in international organizations. Ivana has testified before the European Parliament and has briefed various government officials.

Emily Hester is a research analyst with FDD's Center on Cyber and Technology Innovation, focusing on Russian influence operations and the intersection of emerging technology and national security. She gained experience with a corporate law firm's White Collar Investigations & Defense practice group and has a B.A. in government and Russian area studies from Dartmouth College.

FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the authors do not necessarily reflect the views of FDD, its staff, or its advisors.