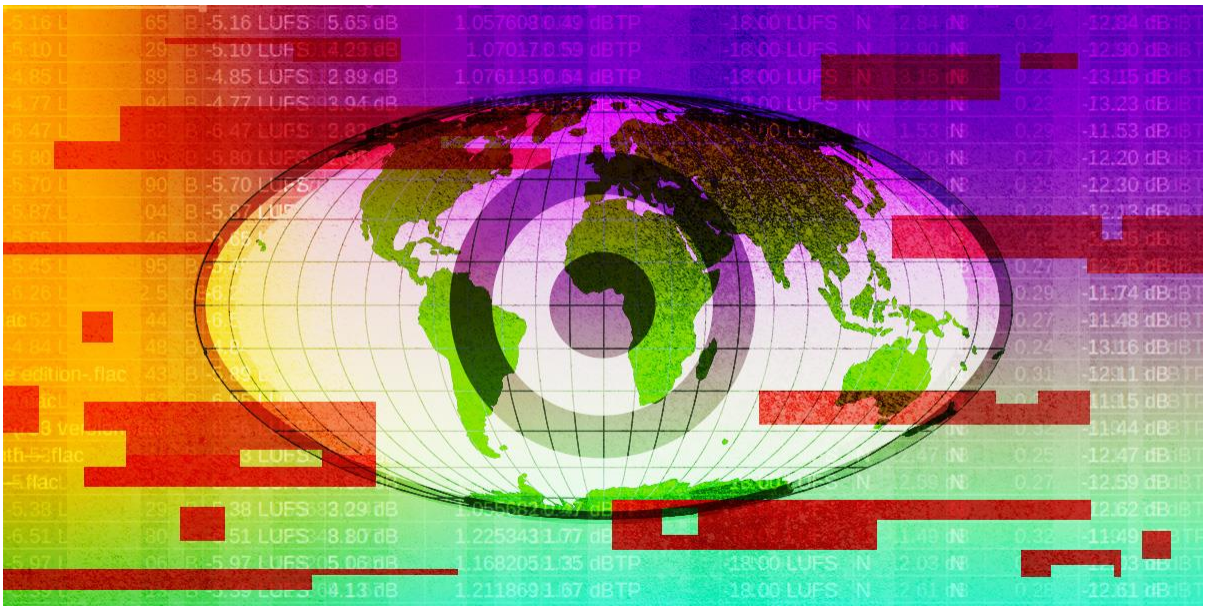

The proposed UN Cybercrime Convention is an extensive surveillance treaty that imposes intrusive domestic surveillance measures and mandates state cooperation in surveillance and data sharing between countries. It includes provisions for mutual legal assistance, requiring states to aid each other in investigations and prosecutions related to cybercrimes, and allows collecting, obtaining, preserving, and sharing of electronic evidence for any crime deemed serious, with little to no human rights safeguards. This cooperation extends even to countries with poor human rights records. Negotiations for this proposed treaty began in 2022, initiated by a controversial proposal from the Russian Federation.

If adopted, the proposed treaty will result in the rewriting of surveillance laws worldwide. Millions of people, including those often targeted by governments for defending human rights, journalists, and those speaking truth to power, will be affected. Without mandatory, clear, and enforceable safeguards, the proposed treaty risks becoming a tool for state abuse and transnational repression rather than a protector of human rights.

EFF's Key Concerns

The Title of the Draft Convention is Misleading and Problematic: Equating cybercrime with any crime committed through ICTs is conceptually and practically harmful. Cybercrime should focus on acts against computer systems, networks, and data. Recent efforts to broaden its definition have led to the criminalization of expression and human rights. On a practical level, equating cybercrime with any

crime committed through ICTs will encourage an expansive interpretation of the treaty, particularly in gray areas of its application.

Insufficient Human Rights Safeguards: Article 24, which addresses conditions and safeguards and includes the principle of proportionality, fails to explicitly include other crucial principles such as legality, necessity, and non-discrimination. Effective human rights protections require judicial approval before conducting surveillance, transparency about actions taken, and notifying users when their data is accessed unless it jeopardizes the investigation. The new draft omits these safeguards, even worse it defers the few existing safeguards to national laws that can vary greatly and may not always provide the necessary protections. It also lacks safeguards for legally privileged information, fails to prevent compelled self-incrimination, and omits protections for criminal defense attorneys. These gaps raise concerns about the erosion of human rights: the treaty doesn't raise the bar against invasive surveillance but rather confirms even the lowest protections, potentially undermining existing robust standards.

Highly Intrusive Secret Spying Powers Without Robust Safeguards: The draft allows for extensive secret surveillance with weak safeguards, posing significant risks both domestically and internationally. It permits real-time interception of traffic data and content for a wide range of offenses, including non-cyber offenses and lawful activities in some countries but criminalized in others. Service providers are compelled to collaborate secretly, making it difficult for public and oversight bodies to monitor and scrutinize these activities effectively. The use of these powers for cross-border assistance in spying and evidence gathering greatly increases the potential for abuse, particularly among countries with diverse human rights records. This cooperation enables the targeting of lawful activities under international human rights standards but criminalized in some nations, exacerbating the risks of transnational repression and human rights abuses.

Broad Scope of the International Cooperation Chapter Remains a Grave Threat: The draft treaty allows one state to assist another in spying on activities considered serious in some countries but legal in others. When both countries criminalize conduct protected by human rights, the treaty legitimizes collaborative abuses.

Risks to LGBTQ and Gender Rights: The broad scope of the convention continues to pose significant risks to LGBTQ+ and gender rights. The international cooperation chapter could be exploited to target individuals based on their gender or sexual orientation, especially if domestic laws criminalize these expressions as serious crimes. This is particularly concerning given the history of cybercrime laws being misused to persecute marginalized groups.

Compelled Technical Assistance: The draft requires countries to have laws enabling authorities to compel anyone with knowledge of a particular computer or device to provide necessary information for access to information, including user identities and personal or location data. This could involve asking a tech expert or engineer to help unlock a device or explain its security features, which may compromise security or reveal confidential information. For example, an engineer might be required to disclose an unfixed security flaw or provide signed encryption keys that protect data.

Expansive Scope and Over-Criminalization Risks: The draft Convention continues to include a wide range of crimes, not just cybercrimes, such as "grooming" and CSAM. The UN's Ad-Hoc Committee Chair overseeing treaty negotiations has added future negotiating sessions to hold talks about including more crimes through a Protocol. This approach continues to unnecessarily broaden the draft Convention's scope, risking over-criminalization of legitimate online activities involving expression and assembly.

Insufficient Protection for Security Researchers and Other Public Interest Work: The draft Convention fails to exempt security research, journalism, and whistleblowing from criminalization, posing significant risks to cybersecurity and press freedom globally. This includes those involved in authorized testing or protection of ICT systems. However, the draft's provisions on illegal access, interception, and interference lack mandatory requirements for criminal intent and harm, threatening to penalize security research efforts.

Want more information? Please contact EFF Policy Director for Global Privacy Katitza Rodriguez at katitza@eff.org.