EFF's Concerns About the UN Draft Cybercrime Convention

The proposed UN Cybercrime Convention is an extensive surveillance pact that imposes intrusive domestic surveillance measures and mandates states' cooperation in surveillance and data sharing. It requires states to aid each other in cybercrime investigations and prosecutions, allowing the collection, preservation, and sharing of electronic evidence for any crime deemed serious by a country's domestic law, with minimal human rights safeguards. This cooperation extends even to countries with poor human rights records. Negotiations for this treaty began in 2022, initiated by a controversial proposal from the Russian Federation. If adopted, it will rewrite surveillance laws worldwide. Millions of people, including human rights defenders, journalists, security researchers, and those speaking truth to power, will be affected. Without clear, enforceable safeguards, the treaty risks becoming a tool for state abuse and transnational repression rather than protecting human rights. Below are our main concerns. For a comprehensive list, please refer to our redlines and appeal to EU Delegates.

EFF's Key Concerns

The Title of the Draft Convention is Misleading and Problematic: Cybercrime is a real issue but equating it with any crime involving ICTs is conceptually and practically harmful. Recent efforts at the domestic level to broaden its definition have led to the criminalization of legitimate activities, such as online criticism, religious expression, or LGBTQ support. In the proposed treaty, it encourages expansive interpretations that could lead to human rights abuses and transnational repression. **Recommendation:** Restrict the definition to "core cybercrimes" like technical attacks on computers, devices, data, and communications systems. Exclude human rights-protected activities from the scope of the treaty to prevent misuse and ensure these rights are not unjustly targeted due to equating cybercrime with any crime using ICT.

Expansive Scope and Over-Criminalization Risks: The draft Convention's criminalization chapter dangerously broadens its scope by including crimes like "grooming" and CSAM, not just cybercrimes. Its CSAM definition risks criminalizing consensual conduct between minors. Even worse, a proposed Protocol could add two more Ad Hoc sessions to discuss even more crimes, further expanding its broad scope. **Recommendation**: Criminalization must be limited to Articles 7 to 11. Narrow the scope of the CSAM article to target only intentional, malicious actions, exclude from criminalization consensual activity between minors, make exemptions for self-generated content by minors mandatory, ensure financing provisions target only those knowingly involved in illegal activities, and exclude the public interest use of such materials, such as evidence in crime investigations, and scientific or artistic materials.

Overbroad Scope of Evidence Gathering Powers Will Enable Domestic and Cross-Border Spying on Acts of Expression: The open-ended scope of Chapters IV & V risks undermining law enforcement cooperation on actual cybercrime offenses by diluting resources. It lets governments spy on people to gather potential evidence for any crime if they've been committed using ICT. It also allows one state to help another in surveillance for any so-called serious crime. These expansions turn the treaty into an extensive surveillance pact. Article 23(2)(c) greenlights invasive measures for minor offenses and protected expressions abusively criminalized in some countries. Article 35(1)(c) means cooperation for serious crimes, defined as offenses punishable by four years or more, which can include acts of expression considered serious offenses in national law. This broad scope risks massive abuse of power. **Recommendation**: Limit Articles 23(2)(c) and 35(1)(c) to Articles 7 to 11 and delete Article 23(2)(b). Support OHCHR's recommendation to revise the definition of serious crimes to mean only "those involving death, injury, or other grave harms," as merely suggesting respect for human rights within such a broad scope is important but insufficient because it lacks enforceable protections against misuse and abuse. Ensure cooperation is limited to situations where there is a reasonable suspicion that legal assistance will produce evidence of a criminal offense.

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 extensive secret surveillance with weak safeguards, posing significant risks both domestically and internationally. Domestically, it permits real-time interception of traffic data for any crime, while content interception is limited to serious crimes—offenses punishable by four years or more in domestic laws. Service providers are compelled to assist in these surveillance activities, often under perpetual gag orders, preventing notification even when investigations are no longer jeopardized. Internationally, the draft allows one state to assist another in carrying out such surveillance for serious crimes, forcing companies to comply with foreign surveillance requests, also in perpetual secrecy. This lack of transparency and accountability is a recipe for unchecked abuses of power and undermines trust in digital services. **Recommendation**: Delete Articles 29, 30, 45, 46.

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 to facilitate access to such system. 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. (ie. an engineer might be arbitrarily required to disclose an unfixed security flaw or provide signed encryption keys that protect data). **Recommendation**: Delete Article 28(4).

Lawless Law Enforcement Cooperation Risks Human Rights Erosion: The current wording of Article 47 risks supporting open-ended law enforcement cooperation without detailing the necessary limitations and safeguards required under international human rights law. States should not use this Convention to authorize or require personal data sharing beyond the scope of existing mutual legal assistance treaties, the safeguards established under the MLA, and the MLA vetting mechanism. Removing these safeguards without providing comparable protections and limitations invites misuse of the mutual legal assistance framework for abuse and/or repression. **Recommendation**: Limit Article 47(1) to Articles 7-11, delete Articles 47(1)(b), (c), and (f), and reference Articles 24 and 36 in Article 47(2).

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. Full list of recommendations available here.

Risks to LGBTQ and Gender Rights: The broad scope of the convention continues to pose significant risks to LGBTQ+ and gender rights. The domestic and 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. **Recommendation**: Restrict the scope of evidence gathering to core cybercrimes. Revise the definition of serious crime as per OHCHR's recommendation.

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