

The UNConventional Cybercrime: How a Bad Anti-Hacking Treaty is Becoming Law

Katitza Rodríguez, Policy Director, Global Privacy
Bill Budington, Senior Staff Technologist

Background

- In the 90s, the **Council of Europe** drafted an international **Convention on Cybercrime** to harmonize cybercrime laws and make international cooperation easier.
- Signed in 2001 in Budapest, so it's called the **Budapest Cybercrime Convention**.
- 130 States (or 67% of UN Member States) currently have substantive criminal law provisions to criminalise offences against and by means of computers "largely in place," like the US Computer Fraud & Abuse Act.



EFF

August 2023

Budapest Cybercrime Convention

- Effective 2004
- "**Additional Protocol**" in 2006 – addressed "racist and xenophobic propaganda."
- "**Second Additional Protocol**" approved in 2022 – focus on expanding law enforcement's cross-border access to data.

- Not just Europe: Sixty-eight countries have ratified.
- Mandates participating countries to adopt **legislation outlawing specified cybercrimes**.
- Defines computer crimes like **illegal access, illegal interception, data interference, system interference, misuse of devices**.

The UN enters the chat

- In December 2019, the UN General Assembly passed Resolution 74/247 and established the **Ad Hoc Committee**.
- Task: “Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose.
  - United Nations Office on Drugs and Crime (UNODC) serves as Secretariat to the AHC.
  - Chair (Algeria) encouraged to get views of “non-governmental organizations, civil society organizations, academic institutions and the private sector.”



Why do we care about Treaties?

- **Treaties are binding** upon signatory countries, who are obliged to comply. Under Article 26 of the aptly named *Vienna Convention on the Law of Treaties*, they become part of international law
- US Constitution provides the President with the “Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two-thirds of the Senators present concur.”
- In US, treaties have the **same force as federal legislation**.
- However often the treaties operate by requiring (*shall*), or making optional (*may*), separate conforming legislation.

Why do we care about Treaties?

- While there are often opportunities to debate how to implement a treaties requirements, key aspects have already been decided.
- This **can short-circuit domestic political processes**. Unless the treaty allows for an exclusion, the country must pass conforming legislation, though the implementation could allow for safeguards.
- This one weird trick has been used to enable bad policy in a variety of areas. For example, the DMCA amends US copyright law to comply with the *WIPO Copyright Treaty* and the *WIPO Performances and Phonograms Treaty*.

What civil society is doing?

- Relevant ”non-governmental organizations, civil society organizations, academic institutions and private sector organizations” were invited to participate in the AHC’s sessions.
- EFF attended all sessions, provided oral statements, policy submissions and amendments, and lobbying Member States.
- Part of our year-long push, along with Privacy International, Human Rights Watch, ARTICLE 19, Access Now, Derechos Digitales, and many other allies, to ensure that human rights are baked into the proposed UN treaty, so it’s not used as a tool to censor legal speech, conduct illegal surveillance, violate privacy rights, or stifle free expression.

Timeframe

- In 2021, the UN General Assembly ordered the Ad Hoc Committee to provide a draft convention for its 78th session (starts **September 2023**);
- Set six sessions to negotiate, from March 2022 to September 2023.
- Concluding session, New York Jan/Feb 2024
- Sixth Session is on August 21 to September 1st in New York.



Should Only Cover Core Cybercrime

Core cybercrimes: illegal access, illegal interception, data interference, computer system interference, and misuse of devices.

Article 17. Offences relating to other international treaties

States Parties shall adopt such legislative and other measures as may be necessary to ensure that offences established in accordance with **applicable international conventions and protocols** also a
through the use of [a computer system]
communications technology devices]



Example – Art. 6 Illegal Access



1. Each State Party shall adopt such legislative and other measures as be necessary to establish as criminal offences under its domestic law, when **committed intentionally**, the access to the whole or any part of [a computer system] [an information and communications technology device] **without right.**

2. A State Party **may** require that the offence be committed **by infringing security measures**, with **the intent of obtaining** [c**omputer data]** [digital information] o**r other dishonest intent or in relation to** [a computer system] [an information and communications technology device] that is connected to another [computer system] [information and communications technology device].

- Provides flexibility in its implementation: Regrettably, still can be interpreted to cover civil disputes (like a TOS or EULA violation); require dishonest intent, which may require "infringing security measures;" major problem: infringing security measures **don't have** to be effective.

Civil disputes are not a crime

- As currently framed, these provisions could threaten t**o elevate private business disputes**, based on rules and terms written by providers, not legislatures, to criminal activity.

- Many cybercrime provisions requires conduct to be otherwise "**without right**," which is not yet **clearly defined**. While the text provides some flexibility "The State m**ay require the offense** to be committed **by infringing a security measure**, it is a "**may**", and not a "shall."

"Under the government's proposed interpretation of the CFAA … posting for sale an item prohibited by Craigslist's policy, or describing yourself as 'tall, dark and handsome' when you're actually short and homely, will earn you a handsome orange jumpsuit."

U.S v. Nosal, 9th Cir (2012)

Civil Society Clarifications

- Many countries' proposals eliminate an intent requirement. **Intent is often the key difference** between a security researcher finding and proving up vulns and a cybercriminal exploiting them.
- These provisions **risk criminalizing the work of security or social researchers**, even when they scan publicly available information since no technical security safeguards needs to be bypassed and no fraudulent or dishonest intent is required
- **Clarify**: Add a requirement for fraudulent or dishonest intent, which will require bypassing effective technical security safeguards; it must be clear that "without right"**cannot turn on violations** of private EULAs, TOS policies or contracts; allow for public interest defense.

EFF

August 2023

Security Research Needs Tools

Lot to parse in Article 10:

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed **intentionally** and **without right**:

(a) The **obtaining**, production, sale, **procurement for use**, import, distribution or otherwise making available of:

(i) A device, including a programme designed or adapted **primarily** for the purpose of committing any of the offences established in accordance with articles 6 to 9 of this Convention; or

(ii) A **password**, access credentials, **electronic signature** or similar data by which the whole or any part of [a computer system] [an information and communications technology device] is capable of being accessed;

with the intent that the device, password, access credentials or similar data be used for the **purpose of committing any of the offences established in accordance with articles 6 to 9 of this Convention**; and

Example: Netflix Sharing

- While passwords are sold criminally for profit, many more are shared by friends and family (without profit), which is more appropriately a civil issue if such action violates the company's Terms of Services.
- For example, Netflix, after years of turning a blind eye to family and friends sharing passwords, is now asking some of the hundreds of millions who share passwords to pay an additional $3.
- As written, this Article could turn millions of ordinary people into “cybercriminals” overnight, all over a three dollar business dispute..



Broader Issues with the Treaty

- Scope. Now it is limited to 11 crimes, some are actual cybercrime and two are CSAM crimes.
- The treaty's procedural powers and international cooperation now raise serious concerns.
- Briefly: Investigative powers required by the Treaty should only be available with respect to crimes covered by the Treaty. The Treaty concerns cybercrime and **should not become a general purpose vehicle** to investigate all crimes.



No Encryption Backdoors



- Article 28. Search and seizure of stored [computer data has a technical assistance provision:

- “Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order **any person who has knowledge about the functioning of the [computer system] [information and communications technology device] in question,** the information and telecommunications network, or their component parts, or measures applied to protect the [computer data] [digital information] therein, to provide, as is reasonable, the necessary information to enable the undertaking of the measures referred to in paragraphs 1 to 3 of this article..”

- Paragraphs 1 to 3 concern government “search or similarly access” of computers and data.

Security is Hard Enough

- Government mandates to help break security won't make things better.
- The "necessary information to enable" a "search or similarly access" to secured computers and data **could be interpreted** to include **assistance in breaking encryption or other security measures**.
- Mandate for vulnerability disclosure?
- Disclosure of private keys?
- New backdoor version?



Where are we now?

- EFF will be attending the sixth session in New York between **August 21 to September 1, 2023.**
- The member states are developing the potential treaty by **proposing language to seek consensus** among the states.
- **EFF and others raised concerns** that draft provisions pose serious threats to free expression, privacy, and the legitimate activities of journalists, whistleblowers, activists, and security researchers.
- We will discuss **drafts**, but **language will keep changing**.



Literally, we were in the UN's Vienna International Centre.



Literally, we'll be in the UN's New York Headquarters on August 21

EFF

Moving Forward

- Sixth session, New York, August 21-September 1, 2023
- Member States will start article-by-article negotiations to reach a consensus on a final draft during a two-week marathon session from August 21 through September 1.
- “Nothing is agreed until everything is agreed”
- Documents from the Session will be available here: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main

Questions

- **Katitza Rodriguez**, Policy Director for Global Privacy
  katitza@eff.org - @txitua
- **Bill Budington**, Senior Staff Technologist
  bill@eff.org

Read EFF.org for updates, or reach out if you have questions.
https://www.eff.org/issues/un-cybercrime-treaty