Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty

February 5, 2024

We, the undersigned, representing a broad spectrum of the global security research community, write to express our serious concerns about the UN Cybercrime Treaty drafts released during the sixth session and the most recent one. These drafts pose substantial risks to global cybersecurity and significantly impact the rights and activities of good faith cybersecurity researchers.

Our community, which includes good faith security researchers in academia and cybersecurity companies, as well as those working independently, plays a critical role in safeguarding information technology systems. We identify vulnerabilities that, if left unchecked, can spread malware, cause data breaches, and give criminals access to sensitive information of millions of people. We rely on the freedom to openly discuss, analyze, and test these systems, free of legal threats.

The nature of our work is to research, discover, and report vulnerabilities in networks, operating systems, devices, firmware, and software. However, several provisions in the draft treaty risk hindering our work by categorizing much of it as criminal activity. If adopted in its current form, the proposed treaty would increase the risk that good faith security researchers could face prosecution, even when our goal is to enhance technological safety and educate the public on cybersecurity matters. It is critical that legal frameworks support our efforts to find and disclose technological weaknesses to make everyone more secure, rather than penalize us, and chill the very research and disclosure needed to keep us safe. This support is essential to improving the security and safety of technology for everyone across the world.

Equally important is our ability to differentiate our legitimate security research activities from malicious exploitation of security flaws. Current laws focusing on "unauthorized access" can be misapplied to good faith security researchers, leading to unnecessary legal challenges. In addressing this, we must consider two potential obstacles to our vital work. Broad, undefined rules for prior authorization risk deterring good faith security researchers, as they may not understand when or under what circumstances they need permission. This lack of clarity could ultimately weaken everyone's online safety and security. Moreover, our work often involves uncovering unknown vulnerabilities. These are security weaknesses that no one, including the system's owners, knows about until we discover them. We cannot be certain what vulnerabilities we might find. Therefore, requiring us to obtain prior authorization for each potential discovery is impractical and overlooks the essence of our work.

The unique strength of the security research community lies in its global focus, which prioritizes safeguarding infrastructure and protecting users worldwide, often putting aside geopolitical interests. Our work, particularly the open publication of research, minimizes and prevents harm that could impact people globally, transcending particular jurisdictions. The proposed treaty's failure to exempt good faith security research from the expansive scope of its cybercrime prohibitions and to make the safeguards and limitations in Article 6-10 mandatory leaves the door wide open for states to suppress or control the flow of security related information. This would undermine the universal benefit of openly shared cybersecurity knowledge, and ultimately the safety and security of the digital environment.

We urge states to recognize the vital role the security research community plays in defending our digital ecosystem against cybercriminals, and call on delegations to ensure that the treaty supports, rather than hinders, our efforts to enhance global cybersecurity and prevent cybercrime. Specifically:

Article 6 (Illegal Access): This article risks criminalizing essential activities in security research, particularly where researchers access systems without prior authorization, to identify vulnerabilities. A clearer distinction is needed between malicious unauthorized access "without right" and "good faith" security research activities; safeguards for legitimate activities should be mandatory. A malicious intent

requirement—including an intent to cause damage, defraud, or harm—is needed to avoid criminal liability for accidental or unintended access to a computer system, as well as for good faith security testing.

Article 6 should not use the ambiguous term "without right" as a basis for establishing criminal liability for unauthorized access. Apart from potentially criminalizing security research, similar provisions have also been misconstrued to attach criminal liability to minor violations committed deliberately or accidentally by authorized users. For example, violation of private terms of service (TOS)–a minor infraction ordinarily considered a civil issue–could be elevated into a criminal offense category via this treaty on a global scale.

Additionally, the treaty currently gives states the option to define unauthorized access in national law as the bypassing of security measures. This should not be optional, but rather a mandatory safeguard, to avoid criminalizing routine behavior such as changing one's IP address, inspecting website code, and accessing unpublished URLs. Furthermore, it is crucial to specify that the bypassed security measures must be actually "effective." This distinction is important because it ensures that criminalization is precise and scoped to activities that cause harm. For instance, bypassing basic measures like geoblocking–which can be done innocently simply by changing location–should not be treated the same as overcoming robust security barriers with the intention to cause harm.

By adopting this safeguard and ensuring that security measures are indeed effective, the proposed treaty would shield researchers from arbitrary criminal sanctions for good faith security research.

These changes would clarify unauthorized access, more clearly differentiating malicious hacking from legitimate cybersecurity practices like security research and vulnerability testing. Adopting these amendments would enhance protection for cybersecurity efforts and more effectively address concerns about harmful or fraudulent unauthorized intrusions.

Article 7 (Illegal Interception): Analysis of network traffic is also a common practice in cybersecurity; this article currently risks criminalizing such analysis and should similarly be narrowed to require criminal intent (*mens rea*) to harm or defraud.

Article 8 (Interference with Data) and Article 9 (Interference with Computer Systems): These articles may inadvertently criminalize acts of security research, which often involve testing the robustness of systems by simulating attacks through interferences. As with prior articles, criminal intent to cause harm or defraud is not mandated, and a requirement that the activity cause serious harm is absent from Article 9 and optional in Article 8. These safeguards should be mandatory.

Article 10 (Misuse of Devices): The broad scope of this article could criminalize the legitimate use of tools employed in cybersecurity research, thereby affecting the development and use of these tools. Under the current draft, Article 10(2) specifically addresses the misuse of cybersecurity tools. It criminalizes obtaining, producing, or distributing these tools only if they are intended for committing cybercrimes as defined in Articles 6 to 9 (which cover illegal access, interception, data interference, and system interference). However, this also raises a concern. If Articles 6 to 9 do not explicitly protect activities like security testing, Article 10(2) may inadvertently criminalize security researchers. These researchers often use similar tools for legitimate purposes, like testing and enhancing systems security. Without narrow scope and clear safeguards in Articles 6-9, these well-intentioned activities could fall under legal scrutiny, despite not being aligned with the criminal malicious intent (*mens rea*) targeted by Article 10(2).

Article 22 (Jurisdiction): In combination with other provisions about measures that may be inappropriately used to punish or deter good-faith security researchers, the overly broad jurisdictional scope outlined in Article 22 also raises significant concerns. Under the article's provisions, security researchers discovering or disclosing vulnerabilities to keep the digital ecosystem secure could be subject to criminal prosecution

simultaneously across multiple jurisdictions. This would have a chilling effect on essential security research globally and hinder researchers' ability to contribute to global cybersecurity. To mitigate this, we suggest revising Article 22(5) to prioritize "determining the most appropriate jurisdiction for prosecution" rather than "coordinating actions." This shift could prevent the redundant prosecution of security researchers. Additionally, deleting Article 17 and limiting the scope of procedural and international cooperation measures to crimes defined in Articles 6 to 16 would further clarify and protect against overreach.

Article 28(4): This article is gravely concerning from a cybersecurity perspective. It empowers authorities to compel "any individual" with knowledge of computer systems to provide *any* "necessary information" for conducting searches and seizures of computer systems. This provision can be abused to force security experts, software engineers and/or tech employees to expose sensitive or proprietary information. It could also encourage authorities to bypass normal channels within companies and coerce individual employees, under the threat of criminal prosecution, to provide assistance in subverting technical access controls such as credentials, encryption, and just-in-time approvals without their employers' knowledge. This dangerous paragraph must be removed in favor of the general duty for custodians of information to comply with lawful orders to the extent of their ability.

Security researchers—whether within organizations or independent—discover, report and assist in fixing tens of thousands of critical Common Vulnerabilities and Exposure (CVE) reported over the lifetime of the National Vulnerability Database. Our work is a crucial part of the security landscape, yet often faces serious legal risk from overbroad cybercrime legislation.

While the proposed UN cybercrime treaty's core cybercrime provisions closely mirror the Council of Europe's Budapest Convention, the impact of cybercrime regimes and security research has evolved considerably in the two decades since that treaty was adopted in 2001. In that time, good faith cybersecurity researchers have faced significant repercussions for responsibly identifying security flaws. Concurrently, a number of countries have enacted legislative or other measures to protect the critical line of defense this type of research provides. The UN Treaty should learn from these past experiences by explicitly exempting good faith cybersecurity research from the scope of the treaty. It should also make existing safeguards and limitations mandatory. This change is essential to protect the crucial work of good faith security researchers and ensure the treaty remains effective against current and future cybersecurity challenges.

Since these negotiations began, we had hoped that governments would adopt a treaty that strengthens global computer security and enhances our ability to combat cybercrime. Unfortunately, the draft text, as written, would have the opposite effect. The current text would weaken cybersecurity and make it easier for malicious actors to create or exploit weaknesses in the digital ecosystem by subjecting us to criminal prosecution for good faith work that keeps us all safer. Such an outcome would undermine the very purpose of the treaty: to protect individuals and our institutions from cybercrime.

Submitted by the Electronic Frontier Foundation, accredited under operative paragraph No. 9 of UN General Assembly Resolution 75/282, on behalf of 124 signatories.

The Full list of signatories supporting this statement is available at this link:
https://www.eff.org/deeplinks/2024/02/protect-good-faith-security-research-globally-proposed-un-cybercrime-treaty