FIFTH INTERSESSIONAL CONSULTATION

UNITED NATIONS AD HOC COMMITTEE ON CYBERCRIME

REMARKS ON CRIMINALIZATION PROVISIONS OF CONVENTION ON CYBERCRIME

June 20, 2023

by Christian Ohanian

Madame Chair and distinguished delegates, my name is Christian Ohanian, I am Senior Counsel for Privacy & Cybersecurity at Mastercard, and I am participating today on behalf of the International Chamber of Commerce (ICC). On behalf of both the ICC and Mastercard, thank you for the opportunity to speak with you today regarding my thoughts on the negotiation of a new Convention on Cybercrime. We appreciate the opportunity to provide a private sector perspective at this final intersessional.

In October 2021, Johnson Memorial Health – a hospital in Indiana - became a victim of a ransomware attack.[1] The human cost of cybercrime followed quickly: ambulances with sick patients were diverted to other hospitals and the hospital staff could not access medical records, losing the ability to leverage the data it relies on to treat patients, including heart rate and blood pressure information. Just a little over a week ago, a German university – the victim of another cyberattack – confirmed that it was forced to take its entire IT infrastructure offline, limiting students' ability to access basic resources for their education, such as the university's library.[2]

As we continue our discussion concerning the elaboration of a new global Convention on Cybercrime, these stories of the direct impact of cybercrime on victims must guide our efforts. When we discuss what conduct should be considered a criminal offense in the new Convention, we must focus on what proposals are the most likely to foster an environment designed to protect victims and ensure the highest level of cyber resilience across our digital ecosystem.

To support the implementation of an effective global framework to enforce cybercrime laws and to deter cyber criminals, the Convention needs to be focused on core cyber-dependent crimes, such as those offenses that relate to the integrity, availability, and confidentiality of an information and communications technologies (ICT) system or device. A narrow focus on these crimes, including "illegal access," "illegal interception," and "interference with an ICT system or device," will enable governments to deploy what are often limited resources toward the most immediate and serious cybercrimes affecting companies and individuals, such as ransomware and distributed denial of service (DDoS) attacks. Emphasizing the enforcement of these cybercrimes will enable governments to leverage broad international consensus to build effective partnerships, including with the private sector.

Each of these crimes should be limited in scope, precisely drawn, and include an element of intent to ensure that they clearly communicate what conduct is prohibited and, thereby, serve as a deterrent to cyber criminals while not discouraging or limiting legitimate and important cybersecurity activities that

---

[1] *See* Farah Yousry, *Cyberattacks on healthcare are increasing. Inside one hospital's fight to recover* (May 8, 2023), NPR, available at: How an Indiana hospital fought to recover from a cyberattack : Shots - Health News : NPR.

[2] *See* Alexander Martin, *Cyberattacks on German university takes 'entire IT infrastructure' offline* (Jun. 12, 2023), RECORDED FUTURE, available at: Cyberattack on German university takes 'entire IT infrastructure' offline (therecord.media).

help protect those who are or might become victims of cybercrime. Specifically, with respect to illegal access (Article 6) and illegal interception (Article 7), these offenses should include a requirement to demonstrate criminal intent, rather than the current language that describes "dishonest intent" as that term is vague and subject to conflicting interpretations.

Conversely, when we consider proposals that stretch far beyond these core cybercrimes – whether they relate to offenses that are focused on the financial sector or the content of speech – governments may inadvertently create an environment that lessens the overall security of our digital ecosystem while also raising human rights and privacy concerns.

Broad concepts of cybercrime can unintentionally undermine the development and use of innovative fraud prevention and cybersecurity solutions – especially where those crimes lack an element of intent. Such cybercrimes can endanger critical cybersecurity activities, including good faith security research, by, among other things, discouraging the collection of certain types of cyber threat data as well as creating an unpredictable legal environment for security research and testing. Even if unintentional, a framework that includes these crimes may have the effect of leaving individuals, companies, and governments with fewer security solutions available to them. With fewer security resources, we will likely see an increase – not decrease – in victims of cybercrime. Therefore, we recommend that the Convention does not treat traditional crime as cybercrime merely because a computer was involved in the planning or execution of the crime. The Convention should include illegal activity that is cyber enabled, only if the offenses are of the scale, scope, or speed that they would not be feasible without ICTs.

Furthermore, attempts to define cybercrime to include offenses relating to the content of speech raise clear human rights and privacy concerns as they may limit freedom of expression and the free flow of data and ideas. What is perhaps less obvious is that such content-based crimes may also create an unpredictable information environment, which can lead to a chilling effect on a range of information sharing, including the sharing of cybersecurity threat information. That information is critical to enabling cybersecurity professionals that are defending against, or recovering from, cyberattacks to be well-equipped to avoid or minimize the operational and economic damage that often follows. A climate that fosters a less open exchange of ideas will be one in which we have less information to defend ourselves and our digital lives.

Finally, it is important to recognize that the decisions governments make concerning how to define offenses subject to enforcement through the new Convention will have a corresponding effect on the outlook for other elements of the treaty that are critical to its effective implementation, such as robust international cooperation and technical assistance. If the Convention embraces a vision of cybercrime that extends beyond the international consensus on core cyber dependent crimes, states may limit their willingness to cooperate in international investigations. And private companies are more likely to encounter exceedingly difficult scenarios, attempting to navigate conflicting legal obligations, including important international obligations that concern privacy and data protection. If the Convention does not narrowly define concepts of cybercrime consistent with a broad consensus, there is also a risk that governments, non-governmental organizations, and the private sector, will be less willing to provide technical assistance to help train those responsible for enforcing such an instrument. With less effective international cooperation and available technical assistance, victims of cybercrime will be left with less information, fewer resources, and inadequate support to defend their networks and recover from a cyberattack. In the same vein, across all these dimensions, dual criminality must be the starting place for

international cooperation on cybercrime. This is fundamental as many elements of cross-border investigative cooperation are greatly limited or rendered ineffective if the criminal acts are not similarly understood in all concerned jurisdictions.

The new draft text of the Convention released last week, which removes many concerning proposals from prior texts, including a number of cyber-enabled and content-based crimes, takes positive steps in the right direction. Nevertheless, with respect to the earlier conversation today regarding Article 17 of the new draft text, we recommend removing this article from the criminalization chapter.

I would like to conclude by thanking you for the opportunity to speak alongside the other stakeholders. A new Convention on Cybercrime could provide an opportunity for enhanced international cooperation in effectively combatting a significant and costly global problem. If that Convention is narrowly focused on core cybercrimes, it will enable the greatest amount of international cooperation while ensuring that our global digital ecosystem is empowered with the tools and resources necessary to defend itself and limit the number of victims.