FOURTH INTERSESSIONAL CONSULTATION

UNITED NATIONS AD HOC COMMITTEE ON CYBERCRIME

Presentation during the Panel **"Technical assistance: setting priorities for the delivery of technical assistance, in particular to developing countries"**

March 6, 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), the institutional representative of 45 million companies of all sizes and sectors in over 100 countries. ICC is committed to ensuring that digital technologies work for everyone, every day, everywhere, to fully realize the potential of the digital economy and to safeguard the proper functioning of critical infrastructure.

On behalf of both ICC and Mastercard, thank you for the opportunity to speak with you today regarding my thoughts on the issue of technical assistance and capacity building as it relates to the negotiation of a new Convention on Cybercrime.

Each day it seems cybercrime finds new victims – whether they are schools, hospitals, governments or businesses. And the cost is growing. By some estimates, the cost of global cybercrime is projected to reach $10.5 trillion annually by 2025.[1] What makes cybercrime so unique is that the devastating effectiveness of a malicious cyber operation is dependent on the borderless nature of the internet and the seamless way our global community interacts each day. A cyberattack suffered in one country is often – if not always – launched from beyond its borders. And its victims can span the globe. That international dynamic requires an international response.

The effort here to build a new Convention to empower a more coordinated and successful effort to fight cybercrime is commendable. But, as we know, without robust international cooperation and technical assistance, the promise of this Convention may not be fully realized.

There are positive signs in recent months from the international community. The newly formed International Counter Ransomware Initiative – a group representing dozens of countries – has committed to, among other things, "[h]old ransomware actors accountable for their crimes and not provide them safe haven," while pledging to coordinate on information sharing and other strategies.[2] Cooperation is just part of the solution. Assistance – in the form of technical assistance and capacity building through training, research and other aspects of support – is necessary if that cooperation has a realistic chance of yielding an effective global system to fight cybercrime.

Governments will, of course, play a central role in providing and facilitating technical assistance and capacity building for States, including for those developing countries that are still building and scaling their capacity to fight cybercrime. The existing relationships between the security services responsible for

[1] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," CYBERCRIME MAGAZINE (Nov. 13, 2020).

[2] International Counter Ransomware Initiative 2022 Joint Statement, THE WHITE HOUSE (Nov. 1, 2022).

cybercrime in various national jurisdictions along with the unique legal authority governments possess to share certain threat information mean that governments will remain critical partners in helping each other build sufficient capacity and capability to fight cybercrime.

At the same time, the private sector has an important role in capacity building as well – one that can complement the unique insights and capabilities of governments.

Today, I'd like to discuss three observations regarding the private sector's role in providing technical assistance and capacity building for States working to bolster their ability to prevent, detect, and fight cybercrime.

First, we know that different countries have different technological capabilities, skills, and expertise. One concerning trend we have witnessed is that, while technical assistance and resources have been increasingly dedicated to support the digitalization of developing countries, corresponding cybersecurity assistance has been lacking. As we know, with the increased digitalization of our daily lives, we increase the surface area that is susceptible to cybercrime. To facilitate effective and tailored technical assistance and capacity building, private companies can help contribute to providing important cybersecurity training to law enforcement agencies, non-profit organizations, and anyone else in a position to help prevent and defend against cybercrime.

Second, private companies can work with governments in carefully calibrated, voluntary public-private partnerships that can foster information sharing and other collaboration.

Finally, to ensure that unexpected roadblocks to cooperation and technical assistance do not impede the effective implementation of the Convention, States should work to ensure that the Convention includes appropriate safeguards for privacy and data protection as well as due process rights.

- **TECHNICAL ASSISTANCE AND CAPACITY BUILDING THROUGH TRAINING**

To start with the question of technical assistance and capacity building, we must remember that the most advanced technology and data lacks any real value without the knowledge and skills to harness it. The current draft chapter of the Convention addressing technical assistance acknowledges the importance of training programs to the successful implementation of the Convention as well as the role of the private sector in contributing to this effort.

While training for law enforcement agencies is a critical component of any effort to build capacity, the most effective way to build lasting capacity to detect and fight cybercrime necessitates building a broader workforce of cybersecurity professionals across industry, academia, and the government.

In the United States alone, nearly a third of all cybersecurity jobs are currently unfilled.[5] Private companies, through their resources and expertise, are in a unique position to help create opportunities to train the next generation of cybersecurity professionals – a workforce that will be critical to building the capacity of states to both prevent cybercrime and investigate it when it occurs.

At Mastercard, for example, we contribute to efforts at all education levels to help facilitate training the next generation of cybersecurity professionals. We created the Cybersecurity Talent Initiative with the help of the Partnership for Public Service, Microsoft, Workday, and U.S. federal agencies – which gives highly qualified students an opportunity to jumpstart their cybersecurity careers by gaining both public sector and private sector work experience. While in Canada, Mastercard has also established a program

to help build the cybersecurity workforce through Mastercard's Global Intelligence and Cyber Centre of Excellence.

These are the types of public and private partnerships that can be leveraged throughout the world to bring private companies and governments together to help train cybersecurity professionals.

In addition to helping build the workforce, the private sector can participate, organize, and help host training exercises alongside governments to facilitate learning about and exchanging the most relevant and cutting-edge skills and expertise.

At Mastercard, we participate in the Cyber Storm Cyber Defense Exercises with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) along with the U.S. Department of Treasury. We also organized and led the first-ever tri-sector Cyber Defense Exercise in the United States, bringing together organizations from energy, finance, and telecommunications to assess cyber-defense capabilities and deepen relationships that will be critical in the event of a real security incident.

We also support non-governmental organizations (NGOs) such as the Global Cyber Alliance (GCA) and the Cyber Readiness Institute (CRI) to increase small business access to cyber solutions. Small businesses are a critical part of our digital ecosystem. And they are often the most vulnerable and least prepared to secure themselves. We aim to work with stakeholders, including governments and other partners, to provide more access to toolkits for small businesses that improve cyber hygiene and strengthen the security of the global supply chain.

With a strong commitment to training and skills development, the private sector, academia, and governments can work together to build capacity that will be resilient and lasting, empowering a generational shift toward a stronger posture to defend against and investigate cybercrime.

- **TECHNICAL ASSISTANCE AND CAPACITY BUILDING THROUGH PUBLIC-PRIVATE PARTNERSHIPS**

Next, we must look to the advantages of carefully calibrated, voluntary public-private partnerships in the fight against cybercrime.

Information and intelligence sharing are important components in providing technical assistance to help prevent and detect malicious cyber activity. Cyber threat information can help organizations understand who may be planning cyberattacks, who may have already perpetrated a cybercrime, as well as help identify the victims. While governments will often be in the best position to provide information concerning these issues, companies can also provide helpful insights where appropriate and consistent with applicable national laws. Strengthened national and international communication between government, law enforcement, and the private sector should be supported by multistakeholder collaboration.

At Mastercard, for instance, we work with the European Cyber Resilience Board, European Cyber Crime and Fraud Investigators, Europol, INTERPOL, and the Financial Services - Information Sharing and Analysis Center (FS-ISAC), among others, to share intelligence and build a more secure digital ecosystem.

Public-private partnership and collaboration can be a critical component of bolstering technical assistance and capacity building around the globe.

- **TECHNICAL ASSISTANCE AND CAPACITY BUILDING WITH SAFEGUARDS**

Finally, it is worth emphasizing that international cooperation between national law enforcement and prosecutorial agencies will be most effective when the scope of the future Convention is clearly and narrowly defined, while including robust safeguards for human rights, privacy, and due process. This could also affect the ability and willingness of private companies to contribute meaningfully to the technical assistance efforts that are critical to making this Convention a success. Clearly and narrowly defining the scope of the Convention to cyber-dependent crimes that are serious, have criminal intent, and are defined similarly across jurisdictions will minimize and avoid conflicts with national laws and existing international instruments, in particular the Budapest Convention, the UN Convention against Transnational Organized Crime (UNTOC) and the UN Convention against Corruption (UNCAC), while building a common understanding of the international rules on cybercrime.

Appropriately tailored privacy, due process, and other protections in the body of the Convention will help provide companies with reassurance when deciding whether to engage with governments and other stakeholders with respect to technical assistance, including training and other partnerships. Without those safeguards, companies will face difficult choices about whether and how to engage in these efforts because of the uncertainty of how that technical assistance or cooperation may be deployed in connection with cybercrime investigations and prosecutions. With the right safeguards, States can foster an environment of healthy collaboration with the private sector to bolster cybersecurity and combat cybercrime.

CONCLUSION

I would like to conclude by thanking you for inviting me to speak alongside these distinguished co-panelists. The work to attempt to implement a global Convention on Cybercrime is a laudable effort that could yield a tremendous tool in the fight against cybercrime. Hopefully, through this process, we can crystalize a plan for technical assistance and capacity building – including a focus on training and public-private partnerships – that will ensure the successful implementation of this Convention.