Statement by the International Chamber of Commerce to the

2nd Intersessional consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

The private sector has, and continues to assume significant roles and responsibilities in the development of information communication technologies. As the representative of 45 million companies of all sizes and sectors in over 100 countries, the International Chamber of Commerce is committed to ensuring that digital technologies work for everyone, every day, everywhere, in order to fully realise the potential of the digital economy and to safeguard proper functioning of critical infrastructures.

ICC works with governments and businesses worldwide to build a common understanding of what constitutes a robust cyber policy in order to foster a more secure Internet for businesses and users.

With a hundred-year history of developing globally recognised applicable rules by convening experts and practitioners, ICC considers it essential that businesses and governments have a shared understanding of how to conceptualise cyber risks, targets, impacts, and responses, including national and international measures.

Malicious cyber activity impacting businesses continues to rise in scale, frequency, and complexity. More than 350 000 new malware variants are released every day, offering hostile cyber actors nearly unlimited options of offensive cyber capabilities.

An increase in ransomware attacks has been further exacerbated by a new model known as Ransomware-as-a-Service, where sophisticated cyber criminals provide easy off-the-shelf access to ransomware tools to any individual or group at low cost.

This has significantly lowered the barriers to entry into this lucrative criminal market, fuelling growth in attacks' complexity and frequency and increasing the potential destructiveness of attacks as inexperienced attackers are given access to extremely sophisticated tools.

Compounding an already daunting situation, threat actors are leveraging the growing complexity of the cyber domain as an opportunity to conduct offensive operations with almost complete deniability.

This ability to operate in increasing obscurity is encouraging a growth in more destructive cyberattacks—incidents are proving to be more costly at a staggering $4.24 million per incident on average in 2021, a 10% year on year increase. Malware such as Wiper (designed to wipe an entire hard drive), the growth in multifaceted attacks (such as a ransomware attack followed by a DDoS attack), and data leakage to force payment are all indicative of increasingly confident cyber adversaries.

Proliferation is compounded by the lack of clear and effective legal and policy counter measures against malicious actors combined with the lack of capacity that law enforcement, judges and other actors of the justice administration organisations have on cyber issues.

This confluence of effects comes at a time when almost 4 million cybersecurity jobs are unfilled globally.

In the face of these continuously growing cyber threats, enforcement itself is not a complete solution: prevention is also key. Prevention efforts can help equip populations with capabilities to defend against risks, they can reduce harm by neutralizing cybercrime attempts and dismantling vulnerabilities before perpetrators succeed in committing offences, and they can also help deter perpetrators from malicious conduct.

The trends I described make it clear that while business investment in prevention and defensive capabilities is essential, the private sector alone is unable to deter, prevent, or properly shield itself (and the communities it helps sustain) from the destructive effects of cybercrime.

As seen with other global security threats, strong international government cooperation, public-private voluntary collaboration, and deterrent measures against cyber criminals and their sponsors are an imperative.

In the context of this Convention let me share four elements that we believe should be in the focus when discussing preventive measures.

1. **Facilitate harmonization of approaches**
   Consistency with existing tools and harmonization of approaches across jurisdictions around the world is essential, especially when combined with initiatives to facilitate faster and more effective coordination between law enforcement agencies.
   Provisions on preventive measures in this Convnetion should ensure consistency with existing UN treaties in the field of crime prevention and criminal justice, in particular the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and take into account multilateral instruments that have already proven their usefulness in the fight against cybercrime, in particular the Council of Europe Convention on Cybercrime – the Budapest Convention.

2. **Recognize and enable multistakeholder cooperation**
   Partnerships are fundamental to successfully prevent cyber threats given the prominent role that the private sectors, computer emergency response teams (CERTs) and non-governmental organizations play in the digital arena. Collaborating with the various actors in the global ecosystem of cybersecurity is of paramount importance to successfully prevent and disrupt cybercrime.
   Governments can take advantage of the expertise and resources of the private sector in the fight against cybercrime. Opportunities include working with industry to share information with enforcement officials about new and emerging threats that technology suppliers experience real-time and that their customers see as priorities. Governments often lack sufficient resources to deal effectively with cybercrime. Working with the private sector can help them achieve greater success, which will help drive trust on both sides, as well as trust of citizens and users in digital technologies overall.
   Collaboration with non-governmental stakeholders can raise public awareness about the threats of cybercrime; ensure the work of governments is undertaken in a transparent manner; and ensure high standards for safeguards such as privacy, civil liberties, and human rights.

3. **Support capacity building**

   The Convention should include provisions on supporting Member States to strengthen their capacity to address cybercrime such as awareness-raising and educational initiatives. This could include provisions to:

   - Support multistakeholder involvement;
   - Encourage collaboration with existing capacity building initiatives to enhance the skills of practitioners and central authorities on their use of technology to facilitate international cooperation in fighting cybercrime, for example the United Nations Office on Drugs and Crime and its Global Programme on Cybercrime or the Global Forum for Cyber Expertise
   - Develop training programmes for law enforcement professionals, investigators and prosecutors and support sharing information and experiences with relevant stakeholders.

4. **The convention as deterrence tool to disincentivize cybercrime**

   As I noted earlier, currently the cybercrime market has a very low entry barrier and promises a very lucrative pay-out, as well as – very sadly – a low probability of getting caught and punished. In this context, defensive measures alone can only go thus far. Defensive measures must go hand in hand with deterring measures, and this convention has the potential to be just that, by providing common definitions of cybercrime, showing shared commitment towards fighting these commonly defined crimes as well as incentivizing collaboration.

   For this to be effective the Convention should focus on cyber-dependent crimes that are serious, have criminal intent, and are defined similarly across the vast majority of member-states. This is fundamental as many elements of cross-border crime cooperation – including prevention – are greatly limited or rendered ineffective if the acts aren't similarly understood in all jurisdictions with a role in addressing the incident.

   At the same time, this convention will only achieve its desired impact if implemented and enforced nationally. National legal regimes must provide states with the tools necessary to effectively combat cyber threats and protect their businesses and communities from an ever-growing ecosystem of threat actors with both political and criminal objectives.

   Turning the tide against escalating cyber conflict will require states to go beyond high-level commitments and focus on their implementation within individual national contexts, going as far as ensuring that malicious criminal actors that break the rules are held accountable.

   A Convention that focuses on cyber-dependent crimes that are serious, have criminal intent, and are defined similarly across jurisdictions has the most potential of becoming ratified and used in practice. This in itself can be an effective preventive tool.