

INTERPOL Statement on Procedural measures and law enforcement

Chairperson, let me thank you for giving us the opportunity to share our views today, and let me also reiterate our commitment to support the important work of the Ad Hoc Committee.

I would like to address the guiding question number 12: on role of the private sector *in supporting law enforcement agencies in preventing and combatting cybercrime*.

The private sector has an instrumental role to play in complementing law enforcement efforts to prevent, detect, investigate and disrupt cybercrime.

When it comes to cybercrime, the majority of data and expertise lies in the hands of the private sector. Some companies hold or have access to global datasets including, imminent threats, long-term or emerging trends, critical intelligence on criminal actors and groups, and modus operandi – all of which are necessary for law enforcement to carry out preventive action, investigations or disruptions such as arrests, searches, and seizures.

We understand that there have been many different views expressed on the relation between national authorities and the private sector in the context of the future Convention and in light of this ongoing debate, INTERPOL wishes to share the model it uses to facilitate collaboration between the law enforcement and the private sector, as a potential way forward.

- In 2019 the INTERPOL General Assembly endorsed a framework called “Project Gateway” with the primary purpose of conducting cybercrime analysis using various sources of information to identify threat actors, victims or compromised infrastructure and take the necessary measures. The “Gateway” framework provides a legal basis for INTERPOL to exchange information with private entities with which it has signed data sharing agreements.
- “Gateway” is underpinned by INTERPOL’s Constitution and its four main principles of **national sovereignty, respect for human rights, neutrality, and active cooperation**.
- Furthermore, INTERPOL’s Rules on the Processing of Data (RPD) set the data protection principles, the conditions under which data may be processed in INTERPOL information systems, as well as rules on the control and monitoring of data processing by INTERPOL member countries, private entities¹ and international entities.
- Through the “Gateway” cooperation model, INTERPOL has been able to establish open, inclusive and diverse partnerships and build greater trust between law enforcement and the private sector. **In particular, these public private partnerships have supported INTERPOL’s ability to rapidly respond to cyber threats and to coordinate joint operations:**
 - (i) **Cybercrime threat response**
 - **First, INTERPOL’s private partners share up-to-date information and expertise on cybercrime trends and threats.**

¹ Art 28 RPD.

- For instance, private-sector partners under Gateway contributed information about emerging cyber threats and the modus operandi of cyber threat actors and groups to INTERPOL's Global Crime Trend Report and regional efforts such as the African Cyberthreat Assessment Reports. These INTERPOL reports enable law enforcement agencies to have a clearer appreciation of the global or regional cybercrime situation so that they can follow up with enforcement action or activities.
- Additionally, the private sector's involvement in INTERPOL's cyber awareness campaigns helps to educate the public and institutions, enhancing their resilience against cyber-attacks.

(ii) Cybercrime operations

- **Second, leveraging on public-private partnerships has enabled INTERPOL to play a leading role in coordinating operational activities, in support of its member countries, to counter cybercrime activities and the actors behind them.**
- For example, in May 2022, INTERPOL received intelligence from several Gateway partners from the private sector (Group-IB, Palo Alto Networks Unit 42 and Trend Micro). The intelligence was enriched by INTERPOL's Cyber Fusion Centre then referred to Nigerian law enforcement, and INTERPOL followed up with multiple case coordination meetings supported by law enforcement in Australia, Canada and the United States. Thanks to this collaborative operation, coordinated by INTERPOL, between the private sector and law enforcement, Nigerian law enforcement were able to successfully apprehend the suspected leader of a transnational cybercrime syndicate responsible for launching mass phishing campaigns and business email compromise schemes.

3. Conclusion :

- In summary, the alliance between private sector and law enforcement is an important part of effectively countering and combating cybercrime at national, regional and global levels. Upholding and deepening this cooperation is vital to maintaining the security and integrity of our shared digital landscape.
- And as a neutral interlocutor between law enforcement and the private sector, INTERPOL stands ready to enable this crucial information flow.