Introduction

The Partnership Against Cybercrime is a group of 50 global organizations and companies that aims to address the global challenge of cybercrime through amplifying public-private cooperation against cybercrime and overcoming barriers to such cooperation.

The Partnership makes this contribution to the ongoing work of the Ad Hoc Committee in addition to any submissions made by its partners and members in their individual capacity. The submission builds on the Partnership’s Insight Report, *Partnership against Cybercrime*.

Public-private partnership in a new international convention

It is important that the new international convention being elaborated by UN member states in the Ad Hoc Committee reflects the reality of how measures to counter cybercrime is conducted in practice and reinforces and promotes the existing public-private cooperation between law enforcement, prosecutorial and judicial authorities and private sector entities. This is in addition to and separate from the more formal requirements states parties may impose on companies when it comes to requests for data and information needed during an investigation.

One of the recurring challenges for public-private collaboration is an unclear and fragmented regulatory environment. This pertains both to how rules and regulations are formulated in national contexts and when working across jurisdictions with different rules. While not explicitly addressing the topic of cybersecurity regulation, the convention still has the potential to enhance harmonization and foster norms for global collaboration against cybercrime. For instance, law enforcement is at times encumbered by rules restricting their contact with private companies.

Highlighting the necessity of collaboration and cooperation with the private sector in the convention would be an important step forward. Nonetheless, the convention can afford states parties with the flexibility on how to encourage such collaboration. Here, inspiration could be drawn from articles 12.2(a) and 39.1 of the United Nations Convention against Corruption (UNCAC), article 31.2(a) of United Nations Convention against Transnational Organized Crime (UNTOC) and preambulatory paragraph 6 of the Council of Europe Convention on Cybercrime.

The Partnership against Cybercrime encourages the Ad Hoc Committee to take these suggestions into account during its work to elaborate a new convention to counter the use of information and communication technologies for criminal purposes.

---

1. Please refer to the Annex for the full list of members.
Connecting public and private organizations to counter cybercrime

When discussing strategies to counter cybercrime, the issue of public-private cooperation and partnership often figure prominently. This is largely because the private sector is in a unique position when it comes to malicious cyber activity. While they are the frontline entities being impacted, they are also well placed to support the fight against cybercrime since their digital infrastructure underpins much of global cyberspace. They have also garnered significant capabilities through dealing with cybercrime in their own organizations. Internet service providers can glean unique insight into global internet traffic and their users’ activities, while cybersecurity companies sit on large amounts of information about the prevailing cyber threats against their clients. In combination, they can enable identification and analysis of cyber threat actors and malicious cyber activities.

For public authorities, such as law enforcement and other judicial and prosecutorial authorities, to be able to prevent, detect, investigate, disrupt and prosecute cybercrime and the cyber threat actors perpetrating them, a close collaboration with these private sector entities is essential. To be successful against cybercriminals, both public institutions and private companies need to forge collaborative partnerships to build on trust and forge a common goal.

To this end, there are several global platforms and initiatives for fostering public-private collaboration, including the Forum’s Partnership against Cybercrime. There is also novel collaboration where law enforcement and private companies work in concert to take coordinated measures in disrupting and dismantling criminal activities. The Forum’s Partnership is currently launching a unique platform called the Cybercrime ATLAS. Through collaboration between several partners, the platform collates knowledge about existing cybercriminal actor groups and their infrastructure.

The Partnership against Cybercrime has formulated several principles for such public-private cooperation to counter cybercrime, including:

- Embracing a shared narrative for collective action against cybercrime
- Cooperating on a basis of long-term strategic alignment
- Undertaking trust-building behaviours
- Systematizing cooperation
- Ensuring value for participation in the cooperation
- Respecting concerns and challenges

3. For example, the INTERPOL Project Gateway that has data-sharing agreements with vetted private sector companies and companies having staff co-located with INTERPOL’s officers as well as Europol’s Joint Cybercrime Action Taskforce (J-CAT) coordinating actions against key cybercrime treats and targets.
Annex: Forum Partnership against Cybercrime members

The World Economic Forum Partnership against Cybercrime consists of the following organizations:

Accenture
Amazon
Banco Santander
Bank of America
Carnegie Endowment for International Peace
Chainalysis
Check Point Software Technologies
Cisco
Cloudflare
Constella Intelligence
Council of Europe
Credit Suisse
Cyber Defence Alliance
Cyber Threat Alliance
Dell Technologies
Deloitte
DXC Technology
Eurojust
European Commission
Europol
EY
Federal Bureau of Investigation
Fortinet
FIRST
Global Forum on Cyber Expertise Foundation (GFCE)

HCL Technologies
International Criminal Police Organization (INTERPOL)
Israel National Cyber Directorate
KPMG
Mastercard
Microsoft
Ministry of Communications and Digitalisation of Ghana
National Crime Agency
NCFTA
Palo Alto Networks
PayPal
PwC
SpyCloud
Standard Chartered Bank
SWIFT
Third Way
Traficura Group
UBS
US Department of Justice
Secret Service
Wipro
World Bank
World Economic Forum
Zurich Insurance Group