DB CONNECT
Stronger Together

BOTTLETOP
#TOGETHERBAND

Bottletop.org / Togetherband.org
@bottletoppers / @togetherbandofficial
Unit 40
7-15 Greatorex Street
London
E1 5NF

DB CONNECT
33 Irving Place
New York, NY 10003
dbconnectnyc@gmail.com

Cybercrime Convention Negotiations TOGETHERBAND’s submission to the Third Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Dear Secretariat and other distinguished members of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies, DB Connect was founded by me, and I serve as the CEO of the company, judge for Grammy winner Pharrell Williams' charitable foundation's $1 million Black Ambition prize competition to fund underrepresented founders, and ambassador for the NGO TOGETHERBAND, a British luxury sustainable brand brought to you by BOTTLETOP. Please accept our sincere gratitude for allowing us to participate in the discussion on prosecuting cybercrime, which we believe is one of the key steps to enhancing international cooperation.

It is understood that the third Ad Hoc Committee session, to be held in August/September, will focus on international cooperation, technical assistance, prevention measures, and implementation mechanisms.

Thus, our submission addresses these areas: (1) the framework of national adjustment; ways to increase international cooperation; streamlined awareness campaigns; the scope and potential objectives of the convention; and (2) the convention's preamble, general provisions, and criminalization provisions. In summary, our recommendations are as follows:

With the creation of more data in the world and the ability to access networks in more ways, cybercriminals are discovering new vulnerabilities to exploit.
The following cybercrime facts and statistics provide an understanding of the cybercrime landscape. With an increasingly digital and connected world, you can see how widespread cybercrime is.

The cost of cybercrime is predicted to hit $10.5 trillion by 2025, according to the latest version of the Cisco/Cybersecurity Ventures "2022 Cybersecurity Almanac." Identity fraud losses tallied a total of $56 billion, according to the "2021 Identity Fraud Study" from Javelin Strategy & Research.

In 2022, the average cost of a data breach has reached a record high of US$4.35 million, according to the 2022 cost of a data breach report by IBM and the Ponemon institute.

COVID-19 accelerated digital transformation and increased dependence on digital services. Data traffic in some markets has increased by 50% due to an increase in telework and social distancing.

Worldwide, cyberattacks have increased during the crisis, including attacks on critical healthcare institutions that were targeted with ransomware. Phishing websites have risen 350% since the start of the pandemic, according to private sector data. Cyber criminals in the United Kingdom and United States have used stimulus packages as the subject of phishing hoaxes in order to exploit the situation for their own personal gain.

Furthermore, due to the increased use of digital tools and services, governments are paying more attention to them. With this opportunity, cyber threats can be addressed and efforts can be unified to ensure a safe, secure, trustworthy, inclusive, and open internet.

Security, privacy, and digital rights can be guaranteed by working together despite the current challenges. These specific actions are needed by governments to maximize this opportunity.

1. **The framework of national adjustment**

Cybersecurity strategies and legal and regulatory frameworks must be updated or developed more quickly by countries. It is imperative that multi-stakeholder initiatives are taken, including a focus on the development of incident response capacities across all sectors. Building effective resilience capabilities requires the participation of the technical community and the private sector.

The harmonization of legislation should also be a priority. The Budapest Convention is the most comprehensive and global agreement dedicated to combating cybercrime today. The agreement has been ratified by 55 countries, and another 10 have requested membership. It is recommended by the Organization of American States (OAS) that countries and organizations adopt the Convention as a means to initiate international cooperation on information sharing and cross-border investigations.

2. **International cooperation should be intensified**.

Information sharing has increased since COVID-19 erupted. We need to maintain this momentum and formalize it for all cyber-related issues. Cybersecurity requires international cooperation, and there is a need to increase trust, at all levels, between countries and industries. Tomorrow, there will be a new "virus" or a "common enemy" in cyberspace; hence, collaboration at the policy, technical, and law enforcement levels will be vital to protect us and allow us to work together to find solutions.

Regional hemispheric networks CSIRTAmericas is an example of international cooperation, comprising computer security incident response teams (CSIRTs) in the Western Hemisphere. In crisis situations such as the Wannacry and COVID-19 pandemics, this community has been able to share real-time information and exchange knowledge and information virtually.

3. **Streamline awareness campaigns**.

It is impossible to be immune to cyber incidents or bad clicks. It is imperative that we raise awareness about cyber incidents at all ages and levels, regardless of industry. A cybersecurity education for children is critical. In this era of rapid technological advancement, children need to immerse themselves in technology at a young age in order to learn the skills they will need throughout their lives. They must be empowered to make the most of this opportunity while also staying protected and aware of their risks.

Governments and the private sector should join together to work toward unified awareness campaigns. There are initiatives such as "Stop. Think. Connect." that could be used as a template for other efforts. Furthermore, users should never be the last line of defense in cybersecurity, as they need to play a role in educating each other and amplifying the reach of awareness campaigns. Cybersecurity is a shared responsibility.

We should also promote a gender-inclusive approach to cyber issues. In the OAS, the Inter-American Commission on Women has already acknowledged the disparate impact of COVID-19 on women's lives, including an increase in internet-based violence against women and girls.

The pandemic's economic impact is disproportionately felt by women, particularly among those without jobs. This reinforces the need to mainstream gender considerations in cybersecurity policies and employment opportunities.

What is Cybersex Trafficking?
Trafficking in cybersex, or online sexual exploitation, is a form of modern slavery and a cybercrime. Victims of cybersex trafficking are coerced, forced, or manipulated into sexual exploitation, and their exploitation is streamed live on the internet through a webcam, video, or photography.

Cybersex trafficking abuses and exploits a growing number of young women and children every year. It is particularly dangerous for impoverished women and girls to be targeted by online traffickers and predators, according to a report by Tear Fund.

Dear Member States, I envisage the following solutions will provide an effective remedy for cybersex trafficking and human rights abuses.

1. Partner with other stakeholders including the private sector, academia, employers, workers' organizations and civil society, to identify and anchor responses to trafficking in persons in the potential presented by technology.

2. The use of technology and innovative tools will enable compliance with the law while safeguarding human rights, including the ability to access justice and full reparation for human trafficking victims.

3. Incorporate appropriate due diligence processes into the design and production of new technologies in an effort to combat the possible use of technology for trafficking.

There is a story behind every #TOGETHERBAND (my NGO). #TOGETHERBAND is brought to you by the British luxury sustainable brand BOTTLETOP. Our bands not only help spread the message of the 17 Sustainable Development Goals and the aim of my NGO Togetherband is to prevent sexual trafficking in Nepal and to give survivors and other disadvantaged women a fresh start after they have been abused.

Non-profit Maiti Nepal emphasizes the importance of its advocacy and intervention programmes, which provide early warning and support to local communities. Through this organization, girls and women are trained in anti-trafficking measures so that strangers who attempt to deceive them with false work offers won't be able to trick them. As part of its mission, Maiti runs mass awareness-raising campaigns in the wider community, builds resource centers, and trains teachers to form anti-trafficking groups.

Following their rescue from trafficking or interceptions at border crossings, girls and women under the care of Maiti Nepal receive shelter and intensive counseling. The purpose of these sessions is to provide individuals with an opportunity to discuss what their interest is in potential employment - for example, tailoring or craft work, which is where #TOGETHERBAND comes into play.

The training is provided to equip women with the skills they need, and we are proud that our #TOGETHERBANDs (mini versions) are made by an established team of artisans in Nepal on a long-term basis, a partnership that gives women the financial independence they need to stay safe.

Yours truly,

Denise Bowen

BOTTLETOP
#TOGETHERBAND