|  |  |
| --- | --- |
|  | **Document CWG-COP-21/INF/1-E** |
| **30 August 2024** |
| **English only** |
|  |  |
| ITU-D Study Group 2 Rapporteur Group Meetings |
| LIAISON STATEMENT ON SECURING INFORMATION AND COMMUNICATION NETWORKS: BEST PRACTICES FOR DEVELOPING A CULTURE OF CYBERSECURITY |
| **Purpose**Below is the liaison statement from ITU-D Study Group 2 Question 3/2 to Council Working Group on Child Online Protection**Action required**This report is transmitted to the Council Working Group on child online protection **for information**.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**References**[*CWG-COP website*](https://www.itu.int/en/council/cwg-cop/Pages/default.aspx)*;* [*SG2RGQ/107*](https://www.itu.int/md/D22-SG02.RGQ-C-0107/) |

|  |  |
| --- | --- |
|  | **Document** [**SG2RGQ/220-E**](https://www.itu.int/md/D22-SG02.RGQ-C-0220/) |
| **21 May 2024** |
| **English only** |
| **Question 3/2:** | **Securing information and communication networks: Best practices for developing a culture of cybersecurity** |
| **SOURCE:** | Co-Rapporteurs for Question 3/2 |
| **TITLE:** | Liaison statement from ITU-D Study Group 2 Question 3/2 to Council Working Group on Child Online Protection |
| **Reference to document:** [**SG2RGQ/107**](https://www.itu.int/md/D22-SG02.RGQ-C-0107/) |

|  |  |  |
| --- | --- | --- |
| Contact: | Name/Organization/Entity: | Ms Vanessa Cravo, Co-Rapporteur for Question 3/2, Brazil |
|  | Phone number: | +55 51 98111 7571 |
|  | E-mail: | vanessac@anatel.gov.br |
| Contact: | Name/Organization/Entity: | Ms Nicole Darabian, Co-Rapporteur for Question 3/2, United Kingdom |
|  | Phone number: | +44 7808 516 769 |
|  | E-mail: | nicole.darabian@ofcom.org.uk  |

**LIAISON STATEMENT FROM ITu-D Study Group 2 Question 3/2
to COUNCIL WORKING GROUP ON CHILD ONLINE PROTECTION**

**ITU-D Study Group 2 Question 3/2:
Securing information and communication networks:
Best practices for developing a culture of cybersecurity**

3 May 2024

|  |  |
| --- | --- |
| **To:** | Council Working Group on Child Online Protection |
| **From:** | ITU-D Study Group 2 (SG2), Question 3/2 |
| **For:** | Information |
| **Approval:** | ITU-D Study Group 2 Question 3/2 Meeting on 3 May 2024 |
| **Contact:** | Ms Nicole Darabian, Co-Rapporteur for Question 3/2, United KingdomE-mail: nicole.darabian@ofcom.org.uk Ms Vanessa Copetti Cravo, Co-Rapporteur for Question 3/2, BrazilE-mail: Vanessac@anatel.gov.brMr Sidy Mouhamed Fall, Vice-Rapporteur for Question 3/2, SenegalE-mail: sidy@primature.sn |
| **BDT Focal Point:** | Mr Orhan Osmani, BDT Focal Point for Question 3/2E-mail: Orhan.Osmani@itu.int |

ITU-D Study Group 2 on Question 3/2 (ITU-D SG2 Q3/2), Securing information and communication networks: Best practices for developing a culture of cybersecurity, sends this liaison statement to the Council Working Group on Child Online Protection (CWG-COP) for information.

ITU-D SG2 [Q3/2](https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/questions/Question-3-2.aspx) would like to thank the CWG-COP for its liaison statement in Document [SG2RGQ/107](https://www.itu.int/md/D22-SG02.RGQ-C-0107/), which was reviewed during the last meeting of Question 3/2 held in May 2024.

COP remains as a highly important topic for Question 3/2, reflecting on the number of contributions received.

Annex 1 of the liaison statement contains summaries and links to contributions on COP‑related issues considered at these meetings.

ITU-D SG2 Q3/2 also looks forward to continuing its collaboration with CWG-COP.

**Annex 1: Brief summary and links to contributions on COP related issues considered at the two ITU-D SG2 Q3/2 RGs meetings** (October 2023 and May 2024)

Document [2/98](https://www.itu.int/md/D22-SG02-C-0098/) (**Australia**): The Australian Government introduced the Online Safety Act 2021 to keep pace with new technology and emerging online harms. The Online Safety campaign aimed to raise public awareness of the Act and the strengthened laws for online safety. The campaign targeted various audience groups and successfully drove traffic to the eSafety Commissioner website. However, the campaign's national reach was limited due to a modest media budget.

Document [2/119](https://www.itu.int/md/D22-SG02-C-0119/) (**Kenya**): The Communications Authority of Kenya (CA) has implemented child online protection initiatives since 2011, focusing on raising awareness and promoting responsible internet usage. The CA has launched two campaigns, "Be The COP" and "Huwezi Tucheza, Tuko Cyber Smart," targeting parents, guardians, teachers, and children. The authority collaborates with various stakeholders, including government agencies, industry players, and NGOs, to implement the ITU Guidelines on Child Online Protection. Initiatives include legal and regulatory frameworks, reporting mechanisms, research and surveys, national strategies, industry initiatives, educational resources, capacity building, and national awareness campaigns.

Document [2/137](https://www.itu.int/md/D22-SG02-C-0137/) (**Côte d'Ivoire**): Côte d'Ivoire faces a digital knowledge gap, hindering its development in the digital world. To address this, public and private sectors, along with international organizations, have launched an awareness campaign for middle and high school students. The campaign aims to educate and raise awareness about online risks, promote responsible digital behaviour, and provide support for reporting abuse. Over 1,000 students participated in the campaign, which emphasizes the importance of a safer digital environment for all citizens.

Document [2/167](https://www.itu.int/md/D22-SG02-C-0167/) (**Australia**): The eSafety Youth Council, established in April 2022, consists of 24 members aged 13-24 from diverse backgrounds in Australia. It aims to involve young people in decision-making processes for policies and programs impacting them. The Council is informed by the Western Sydney University Youth Engagement Report and follows six Best Practice Principles. Members engage in various activities, including conferences, resource launches, and discussions with tech companies. The Council's priorities include collaboration, improved reporting processes, age-appropriate content access, and increased engagement on online safety.

Document [SG2RGQ/114 + annex](https://www.itu.int/md/D22-SG02.RGQ-C-0114/) (**Zambia**): This document summarizes Zambia's dedication to child online safety by adopting ITU Resolution 179 and executing a National COP Strategy, focusing on legal frameworks, education, combating exploitation, stakeholder cooperation, and ensuring effective oversight.

Document [SG2RGQ/130](https://www.itu.int/md/D22-SG02.RGQ-C-0130/) (**Réseau International des Femmes Expertes du Numérique (RIFEN)**): This document outlines Côte d'Ivoire's cybersecurity strategies, including the Platform for Combating Cybercrime and CI-CERT, stressing public awareness and education to foster a cybersecurity culture and safeguard the online space, particularly during events like the African Cup of Nations.

Document [SG2RGQ/165](https://www.itu.int/md/D22-SG02.RGQ-C-0165/) (**Brazil**): This document summarizes Anatel's 2023 Strategic Planning, highlighting digital transformation and meaningful connectivity, which encompasses a cyber safety perspective. It details cyber hygiene initiatives, including the launch of a dedicated page to combat digital scams and frauds.

Document [SG2RGQ/170](https://www.itu.int/md/D22-SG02.RGQ-C-0170/) (**Russian Federation**): This document outlines Russia's "Digital Economy" program for human capital and economic growth by 2024, including "Digital Literacy Campaign" with partners like Kaspersky Lab to educate children on digital safety through animated videos.

Document [SG2RGQ/212](https://www.itu.int/md/D22-SG02.RGQ-C-0212/) (**China Mobile Communications Co. Ltd (China)**): This document presents the critical nature of cybersecurity for Chinese minors, addressing their high online presence, urban-rural digital divide, and exposure to risks like addiction and privacy violations. It underscores China's advancements in safeguarding minors' Internet use and the collective role of government, industry, and society in bolstering cyber-security education and safety.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_