

Australia's Statement

Technology is at our fingertips. As its benefits continue to grow, we need to have, and maintain, a deep understanding of the criminal elements that will exploit technology and do us harm. The modes and methods of cybercrime are not static. They evolve relentlessly, with cybercriminals always probing for weaknesses in capability or resolve. This was evident in the rapidity with which cybercriminals leveraged the COVID-19 pandemic.

In the face of this mutating transnational threat, the importance of the IEG as a platform for sharing our expertise and our experiences should not be underestimated.

Australia wishes to reaffirm the centrality of international cooperation in combatting cybercrime. As technology draws people and networks ever tighter, each of us in the international community must rely on our neighbour to prevent, investigate and prosecute cybercrime. This chain of reliance is only as strong as its weakest link.

None of us can afford to be that link. We must move forward together and with determination.

Australia urges the IEG to recommend that the international community prioritise the provision of capacity building and other support to strengthen the ability of national authorities to respond to cybercrime. Prioritising resourcing and building expertise within national authorities to detect, investigate, and prosecute cybercrime is critical if we are to be effective in combatting cybercrime. .

Australia is proud of its record partnering with others to improve cybercrime capability in our region. Australia takes a multifaceted approach to capability building—supporting our regional partners to tackle technical, legal and operational barriers to their cybercrime response. For example, Australia, the Council of Europe and private sector partners worked closely with Tonga on law reform and technical assistance to help it become the first Pacific Island country to accede to the Council of Europe Convention on Cybercrime in 2017.

The hard-won spirit consensus and cooperation on crime prevention and criminal justice matters must prevail as we approach new international legal frameworks for cybercrime, pursuant to General Assembly Resolution 74/247. Australia calls for a transparent, inclusive and consensus-based treaty making process, informed by the findings and recommendations of the IEG.

Given the rapidly evolving nature of cybercrime, it is crucial that this expert driven forum for technical exchange continues.

Australia invites the Commission on Crime Prevention and Criminal Justice to decide a work program for the IEG to conduct a comprehensive study on cybercrime beyond the 2021 stocktaking meeting, including an examination of approaches to child sexual abuse and exploitation online and other emerging forms of cybercrime.