

New Zealand Written Comments: Intergovernmental Expert Group on Cybercrime April 2021

New Zealand is pleased to respond to note verbale CU 2021/108(A)/DTA/OCB/CSS regarding the compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in 2018, 2019 and 2020. We are also pleased to provide written comments on that topic, as well as the future work of the Expert Group, ahead of the development of conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice.

New Zealand would like to acknowledge the work of participants in the Expert Group and the value of the discussions that have been had in this forum.

Cybercrime is borderless and it therefore follows that international cooperation is essential if we are to effectively address it. Law enforcement agencies need to be able to cooperate with partners in other countries to investigate and prosecute serious crime. Such cooperation addresses a pressing problem for all of us and New Zealand believes we should all work to bolster it.

The work of the Intergovernmental Expert Group is very important in this regard. Having a fora for experts and practitioners to pool their collective experience and expertise is highly valuable. This allows us all to learn from one and other and become more effective at preventing and countering cybercrime.

Since the last IEG session in 2020, New Zealand has been invited to accede to the Budapest Convention on Cybercrime, and confirmed its intention to do so. We consider the Budapest Convention is a strong and effective framework for international cooperation to address online crime and other serious crime involving electronic evidence, in a way that supports a free and open internet and human rights online.

Recommendations

With regard to specific recommendations that we want to see reflected in the conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice, New Zealand would like to provide some thoughts for consideration:

- Firstly, New Zealand is strongly of the view that the IEG's report must remain tightly focused on issues that fall within the UNODC's mandate. In other words, focussed on the appropriate scope of cybercrime, rather than unnecessary duplication with other processes. There is no shortage of important work for us to focus on within the cybercrime context and we believe the IEG's report and recommendations will be stronger if they remain squarely focused on relevant matters. In that vein, we request that the final report does not make any conclusions or recommendations in the areas that fall outside the scope of the UNODC's work, for example references to critical infrastructure protection, use of force, and rules, principles and norms of responsible state behaviour in cyberspace are not appropriate in this fora.

- Secondly, we believe the recommendations and conclusions should be action-oriented and practical. It is only if they are framed in this way that the recommendations will have a genuine impact on our significant shared challenge.
- New Zealand considers the report should highlight the importance of ensuring domestic legislation allows for effective lawful access to evidence of serious crimes, so that international cooperation can occur between law enforcement agencies. It should also reinforce that domestic legislation should be grounded in appropriate safeguards including around human rights, privacy, due process and rule of law, taking into consideration existing international frameworks.
- New Zealand sees it as extremely important that capacity building is highlighted in the report. It is only through technical capability-building we can help ensure all states are able to address cybercrime and cyber-enabled crime. States could be encouraged to lift efforts and build law enforcement cooperation effort in this area. The UNODC should cooperate closely with other organisations, including regional organisations, in the field of capacity building. It is important that initiatives do not duplicate existing efforts or further fragment efforts.
- As in other areas of cyberspace, cybercrime needs to be addressed through a multi-stakeholder lens. We think the conclusions and recommendations should reflect that wide stakeholder involvement and public-private partnerships are essential if our efforts are to be effective.
- New Zealand would like the recommendations to highlight the value of existing international treaties enabling mutual legal assistance and international cooperation on cybercrime and cyber-enabled crime, and that future work should build on what has already been agreed.
- International cooperation on cybercrime relies on both formal, treaty-based cooperation and traditional police-to-police assistance; both need to be recognised in the recommendations. This includes the value of establishing, and using, relevant points of contact to facilitate cooperation on what are often fast-moving issues.
- When considering how to approach the question of a new instrument on cybercrime, New Zealand remains of the view international discussions should remain focused on delivering practical and concrete outcomes aimed at preventing, detecting and responding to cybercrime rather than to expend energy on new instruments. Nevertheless, New Zealand will engage constructively in the Ad Hoc Committee format but it is important that any recommendations relating to this in the IEG report note that such an instrument should not conflict with existing instruments, which already enable international cooperation, and that an instrument must promote a free, open and secure internet and promote and protect the application of human rights online.
- New Zealand's strong view is that it is important that the conversations of the type facilitated by the IEG continue in Vienna. Cooperation at the expert level are highly valued and will not be able to occur within the parameters of the AHC discussions on a convention on cybercrime.