New Zealand National Statement: Cybercrime Intergovernmental Experts Group 27 July 2020

This group meets in extraordinary and challenging circumstances. Collectively, we are confronted by a pandemic which has affected almost every aspect of daily life in nearly every country in the world.

As we come together in this context, effectively cooperating to tackle cybercrime has taken on a new significance. New Zealand has publicly expressed concern about malicious cyber activity that seeks to take advantage of the pandemic. As work, research, commerce, and social interactions shift increasingly online, the attack surface for cyber criminals increases. Malicious actors are preying on the public's curiosity and anxiety about the pandemic, using COVID-19 themed lures for phishing attacks. Some actors are even targeting infrastructure central to the response to the pandemic – a deplorable act especially in the current environment.

This underscores the criticality of the work of the IEG, and the importance of international cooperation in this space. Addressing cross-boundary issues such as these require international solutions. And such cooperation addresses a pressing problem for all of us.

New Zealand is pleased to share with the group that we have expressed interest in acceding to the Council of Europe Convention on Cybercrime (the Budapest Convention), and have launched an associated public consultation process. New Zealand acknowledges the Budapest Convention as 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.

We are particularly concerned about cybercrime in our region, affecting both New Zealand and our close partners in the Pacific. In September 2019 New Zealand announced a $10 million programme of capacity-building support on cyber security for Pacific Island Countries. One pillar of this support is dedicated to combatting cybercrime. We look forward to working with our Pacific partners as we roll this programme out, including in the context of the Pacific Islands Forum's Boe Declaration on Regional Security, which includes cybercrime as a strategic focus area.

We note that, since this group last met, there have been developments in the Third Committee of the UN that have added another dimension to the international cybercrime conversation – namely, the passing of resolution A/RES/74/247 establishing an Ad Hoc Committee to take forward discussions on a UN convention on cybercrime.

New Zealand remains of the view that the international community already has existing mechanisms, such as the Budapest Convention, and the discussions happening in this Group, to enhance international cooperation on cybercrime. In general, our preference is

that international discussion remains focused on delivering practical and concrete outcomes aimed at preventing, detecting and responding to cybercrime, rather than to expend further resource on developing new instruments.

New Zealand welcomes and benefits from international cooperation on effective lawful access to evidence of serious crimes worldwide, including with respect to improving mutual assistance processes. New Zealand also considers that anti-money laundering and countering the financing of terrorism measures, as well as asset recovery measures, need to be a strong part of the law enforcement response to cybercrime.

Nevertheless, New Zealand will engage in the Ad Hoc Committee in a constructive way, with a view to promoting discussions that take account of progress the international community has already made on these issues; that promote a free, open and secure internet; and that promote and protect the application of human rights online.

In taking forward the work of the Ad Hoc Committee, we urge states to consider how we can ensure discussions are inclusive, are transparent, and give the best chance for consensus. We also wish to reaffirm the important role we see for the IEG in international cybercrime cooperation, and note the value in the Ad Hoc Committee beginning substantive deliberations only after this Group has produced its report.

With respect to specific recommendations, we suggest the IEG acknowledges:

- The value of existing international treaties enabling mutual legal assistance and international cooperation on cybercrime, and conventions enabling mutual assistance and international cooperation on the connections between cybercrime, anti-money laundering, and asset recovery;
- 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, with appropriate safeguards;
- The value of technical capability-building to ensure 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 benefit of establishing and using, at both policy and operational level, relevant points of contact to facilitate cooperation on what are often fast-moving issues;
- The importance of a free and open internet, and application of human rights online;
- The importance of multi-stakeholder engagement in addressing cybercrime.

New Zealand looks forward to continuing to work with all states to address this pressing international issue.

ENDS